TP-LINK®

User Guide

TL-WA7510N

5GHz 150Mbps Outdoor Wireless Access Point



Rev: 1.0.0
1910010534

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2011 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

FCC STATEMENT



This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 35 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning



This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

TP-LINK® TP-LINK TECHNOLOGIES CO., LTD

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **5GHz 150Mbps Outdoor Wireless Access Point**

Model No.: **TL-WA7510N**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC

The above product is in conformity with the following standards or other normative documents

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN60950-1:2006

Recommendation 1999/519/EC

EN62311:2008

Directives 2004/108/EC

The above product is in conformity with the following standards or other normative documents

EN 55022:2006 +A1:2007

EN 55024:1998+A1:2001+A2:2003

EN 61000-3-2:2006

EN 61000-3-3:1995+A1:2001+A2:2005

Directives 2006/95/EC

The above product is in conformity with the following standards or other normative documents

EN60950-1:2006

Directive（ErP） 2009/125/EC

Audio/Video, information and communication technology equipment- Environmentally conscious design

EN62075:2008

Person is responsible for marking this declaration:



Yang Hongliang
Product Manager of International Business

TP-LINK TECHNOLOGIES CO., LTD.
South Building, No.5 Keyuan Road, Central Zone, Science & Technology Park, Nanshan, Shenzhen, P. R. China

CONTENTS

Package Contents **1**

Chapter 1 Introduction **2**

1.1 Product Overview 2

1.2 Conventions 2

1.3 Main Features 2

1.4 Panel Layout 3

1.4.1 The Rear Panel 3

1.4.2 The Front Panel 4

Chapter 2 Connecting the Device **5**

2.1 System Requirements 5

2.2 Installation Environment Requirements 5

2.3 Connecting the Device 5

2.3.1 Standard AP Mode 5

2.3.2 AP Router Mode 9

2.3.3 AP Client Router Mode 10

Chapter 3 Quick Installation Guide **11**

3.1 Configuring the PC 11

3.2 Quick Setup 14

3.2.1 Standard AP Mode 16

3.2.2 AP Router Mode 27

3.2.3 AP Client Router Mode 30

Chapter 4 Configuring Standard AP Mode **33**

4.1 Login 33

4.2 Status 34

4.3 Quick Setup 35

4.4 QSS 35

4.5 Operation Mode 41

4.6 Network 41

4.7 Wireless 42

4.7.1 Wireless Settings 43

4.7.2 Wireless Security 43

4.7.3 Wireless MAC Filtering 55

4.7.4 Wireless Advanced 57

4.7.5 Antenna Alignment 59
4.7.6 Distance Settings 59
4.7.7 Throughput Monitor 60
4.7.8 Wireless Statistics 60
4.8 DHCP 61
4.8.1 DHCP Settings 62
4.8.2 DHCP Clients List 63
4.8.3 Address Reservation 63
4.9 System Tools 65
4.9.1 SNMP 65
4.9.2 Diagnostic 67
4.9.3 Ping Watch Dog 68
4.9.4 Speed Test 69
4.9.5 Firmware Upgrade 70
4.9.6 Factory Defaults 71
4.9.7 Backup & Restore 72
4.9.8 Reboot 72
4.9.9 Password 73
4.9.10 System Log 74
Chapter 5 Configuring AP Router & AP Client Router Mode 75
5.1 Login 75
5.2 Status 76
5.3 Quick Setup 79
5.4 QSS 79
5.5 Operation Mode 85
5.6 Network 85
5.6.1 LAN 86
5.6.2 WAN 86
5.6.3 MAC Clone 96
5.7 Wireless 97
5.7.1 Wireless Settings 97
5.7.2 Wireless Security 103
5.7.3 Wireless MAC Filtering 105
5.7.4 Wireless Advanced 108
5.7.5 Antenna Alignment 109

5.7.6 Distance Settings 110
5.7.7 Throughput Monitor 110
5.7.8 Wireless Statistics 111
5.8 DHCP 112
5.8.1 DHCP Settings 113
5.8.2 DHCP Clients List 114
5.8.3 Address Reservation 114
5.9 Forwarding 116
5.9.1 Virtual Servers 116
5.9.2 Port Triggering 118
5.9.3 DMZ 121
5.9.4 UPnP 122
5.10 Security 123
5.10.1 Basic Security 123
5.10.2 Advanced Security 124
5.10.3 Local Management 126
5.10.4 Remote Management 127
5.11 Parental Control 128
5.12 Access Control 130
5.12.1 Rule 130
5.12.2 Host 132
5.12.3 Target 133
5.12.4 Schedule 134
5.13 Static Routing 136
5.14 Bandwidth Control 137
5.14.1 Control Settings 137
5.14.2 Rules List 138
5.15 IP& MAC Binding 138
5.15.1 Binding Settings 139
5.15.2 ARP List 140
5.16 Dynamic DNS 140
5.17 System Tools 144
5.17.1 Time Settings 144
5.17.2 Diagnostic 145
5.17.3 Firmware Upgrade 147
5.17.4 Factory Defaults 148

5.17.5 Backup & Restore 149
5.17.6 Reboot 149
5.17.7 Password 150
5.17.8 System log 151
5.17.9 Statistics 153
Appendix A: FAQ 155
Appendix B: Factory Defaults 160
Appendix C: Specifications 161
Appendix D: Glossary 162

Package Contents

The following items should be found in your package:

- One TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point
- One Power Injector
- Ethernet Cable
- One Power Adapter for TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point
- Mounting Kits
- Quick Installation Guide
- One Resource CD for TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point, including:
 - This User Guide
 - Other helpful information

Note:

Make sure that the package contains the above items. If any of the listed items is damaged or missing, please contact with your distributor.

Chapter 1 Introduction

1.1 Product Overview

The TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point is dedicated to outdoor wireless network solutions. The TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point will allow you to connect your network with other wireless devices wirelessly, sharing Internet Access, files and fun, easily and securely. The high power design will also help you build a more stable link or cover more area outdoors.

The TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point provides three operation modes for multi-users to access the Internet: Standard AP, AP Router and AP Client Router. In Standard AP mode, it can work in various modes, such as Access Point/Multi-SSID/Client/Repeater/Universal Repeater/ Bridge with AP. In AP Router mode, it can access the Internet via an ADSL/Cable Modem, while sharing data wirelessly. In AP Client Router mode, it works as a WISP CPE and can access the Internet wirelessly via your WISP.

With the most attentive wireless security, the TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The AP provides wireless LAN 64/128/152-bit WEP encryption security, and WPA/WPA2 and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

The TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point complies with the IEEE 802.11a, IEEE 802.11n standards so that the data transmission rate is up to 150 Mbps. The wireless transmission range can extend up to tens of kilometers.

1.2 Conventions

The AP, TL-WA7510N, or Device mentioned in this User guide stands for TL-WA7510N 5GHz 150Mbps Outdoor Wireless Access Point without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation. You can set the parameters according to your demand.

1.3 Main Features

- Complies with IEEE 802.11a, IEEE 802.11n, IEEE 802.3, IEEE 802.3u, IEEE 802.1x, IEEE 802.3x, IEEE 802.11i, IEEE 802.11e
- Wireless Data transfer rates up to 150 Mbps
- Supports Standard AP, AP Router and AP Client Router operation mode
- High output transmit power and receive sensitivity optimized

- Supports AP Client Router Mode for WISP CPE
- Supports passive power over Ethernet
- Supports Wireless Distribution System (WDS)
- Supports Antenna Alignment
- Provides throughput monitor indicating the current wireless throughput
- Supports Layer 2 User Isolation
- Supports Ping Watch Dog
- Supports link speed test
- Supports Remote Management
- Output transmit power adjustable
- Supports PPPoE, Dynamic IP, Static IP, L2TP, PPTP and BigPond Cable Internet Access (BigPond Cable Internet Access is only available in AP Router mode.)
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through
- Supports Virtual Server, Special Application and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Provides WLAN ACL (Access Control List)
- Supports configuration backup/restore and firmware upgrade
- Supports Web management

1.4 Panel Layout

1.4.1 The Rear Panel

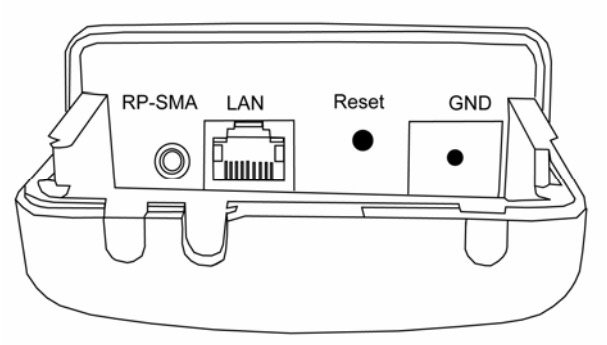


Figure 1-1 Rear Panel sketch

View from left to right, the parts are explained below.

- **RP-SMA:** This is where you can connect an outside antenna. For this AP, the antenna is built inside, and usually there is no necessity to connect an outside one.
- **LAN:** This port is used to connect to the POE port of the provided Power Injector.
- **Reset:**

 There are two ways to reset the AP's factory defaults:

 - Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the AP's Web-based Utility.
 - Use the Factory Default Reset button: Press and hold the **Reset** button until **Wireless Signal Strength** LEDs flash, and then the AP will reboot.

Note:

Ensure the AP is powered on before it restarts completely.

1.4.2 The Front Panel

TL-WA7510N consists of several LED indicators, which is designed to indicate connections and wireless signal.

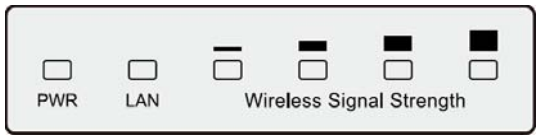


Figure 1-2 Front Panel sketch

View from left to right, the details are explained below.

Name	Status	Indication	
PWR	Off	No Power	
	On	Power on	
LAN	Off	There is no device linked to the corresponding port	
	On	There is a device linked to the corresponding port but no activity	
	Flashing	There is an active device linked to the corresponding port	
Wireless Signal Strength	Off	There is no remote wireless signal	Client or Repeater mode
	On	Indicates the wireless signal strength of a remote AP	

Table 1-1 the LED Description

Chapter 2 Connecting the Device

2.1 System Requirements

- Each PC in the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- TCP/IP protocol must be installed on each PC.
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later.
- If the device is configured to AP client router mode, you also need:

 Wireless Internet Access Service (WISP).
- If the device is configured to AP router mode, you also need:

 Broadband Internet Access Service (DSL/Cable/Ethernet).
- One DSL/Cable Modem that has an RJ45 connector (you do not need it if you connect the router to the Ethernet.).

2.2 Installation Environment Requirements

- Operating temperature: -30℃~70℃
- Operating Humidity: 10%~90% RH, Non-condensing

2.3 Connecting the Device

To connect the AP, please follow the steps below:

1. Power off your PC, Cable/DSL Modem, and the AP.
2. Locate an optimum location for the AP. The best place is usually at the center of your wireless network. The place must accord with the Installation Environment Requirements.
3. Adjust the direction of the antenna. Normally, upright is a good direction.

After finishing the steps above, please choose the operation mode you need and carry out the corresponding steps. There are three operation mode supported by this AP: **Standard AP**, **AP Router**, **and AP Client Router**.

2.3.1 Standard AP Mode

In this mode, the device enables multi-users to access, and provides several wireless modes, including Access Point, Multi-SSID, Client, Repeater, Universal Repeater, and Bridge with AP. These six modes are illustrated as below:

- **Access Point**

This operation mode allows wireless stations to access.

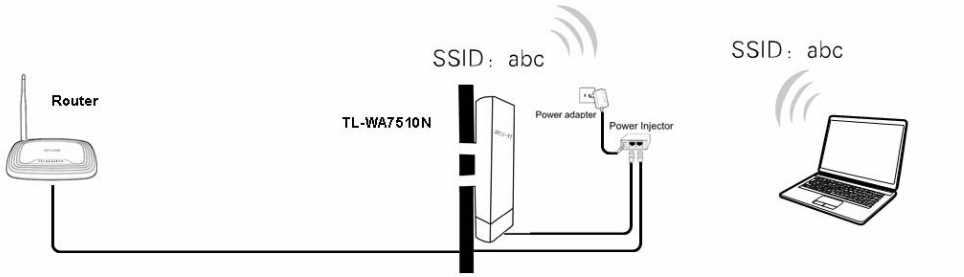


Figure 2-1 Hardware Installation of the TL-WA7510N in Access Point mode

1. Connect the LAN port of TL-WA7510N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the LAN port of the Power Injector to the wired network port with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in the electrical wall socket.
4. Power on the notebook(s) and other connected devices (such as the Router).

- **Multi-SSID**

In this mode, AP can support up to 4 SSID.

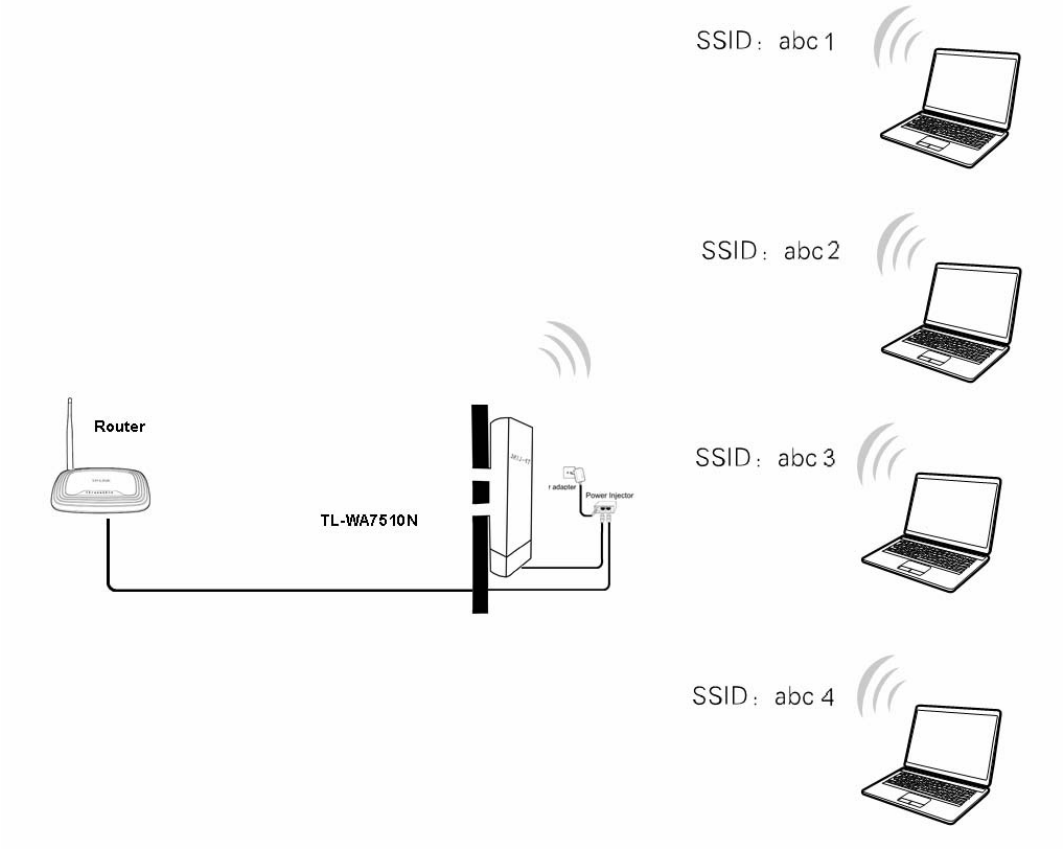


Figure 2-2 Hardware Installation of the TL-WA7510N in Multi-SSID mode

1. Connect the LAN port of TL-WA7510N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the LAN port of the Power Injector to the wired network port with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in the electrical wall socket.
4. Power on the notebooks and other connected devices (such as the Router).

- **Client**

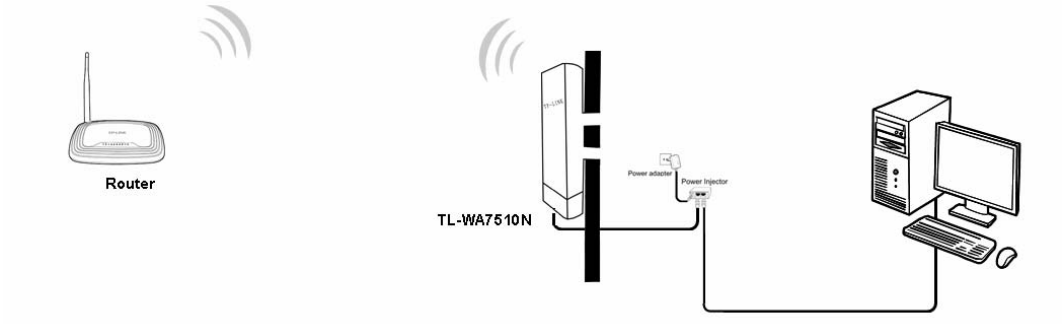


Figure 2-3 Hardware Installation of the TL-WA7510N in Client mode

1. Connect the LAN port of TL-WA7510N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the PC to the LAN port of the Power Injector with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
4. Power on the PC(s) and other connected devices (such as the Router).

➢ **Repeater and Universal Repeater**

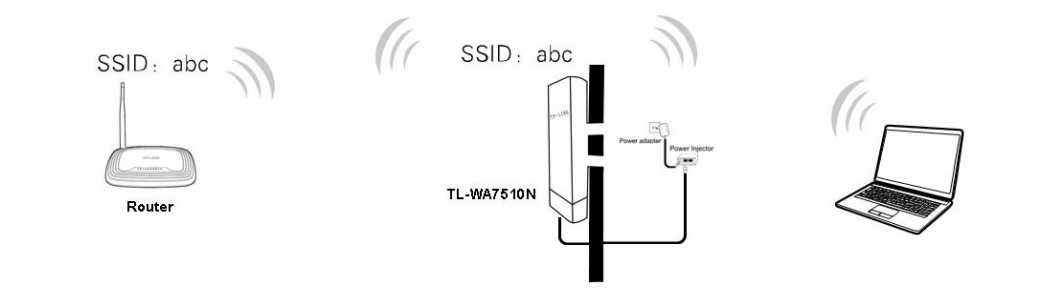


Figure 2-4 Hardware Installation of the TL-WA7510N in (Universal) Repeater mode

1. Connect the LAN port of TL-WA7510N to the POE port of the Power Injector with an Ethernet cable.
2. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
3. Power on the PC(s) and other connected devices (such as the Router).

☞ **Note:**

Both Repeater and Universal Repeater modes allow the AP with its own BSS to relay data to a root AP. The wireless repeater relays signal between its stations and the root AP for greater wireless range. However, in Repeater mode, the WDS associated is enabled, while in Universal Repeater mode, the WDS associated is disabled.

➢ **Bridge with AP**

Two Devices are needed in this mode.

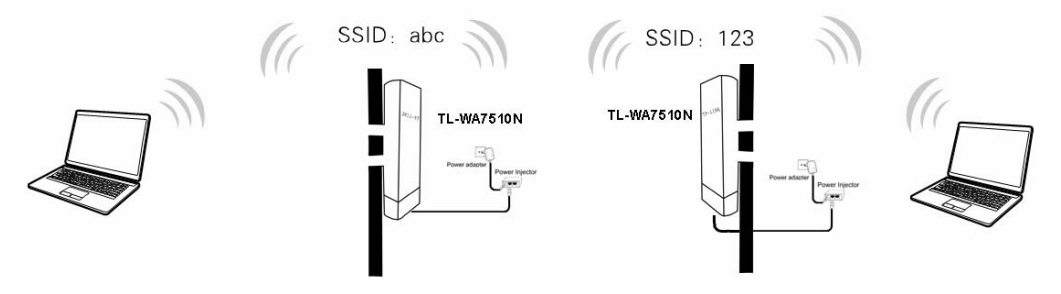


Figure 2-5 Hardware Installation of the TL-WA7510N in Standard AP -- Bridge mode

1. Connect the LAN port of TL-WA7510N to the POE port of the Power Injector with an Ethernet cable.
2. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
3. Power on the PC(s).

Note:

It is recommended that you connect a PC/notebook to the LAN port of the Device with an Ethernet cable, and then login the Device from the PC/notebook to set the Device in Bridge with AP mode.

2.3.2 AP Router Mode

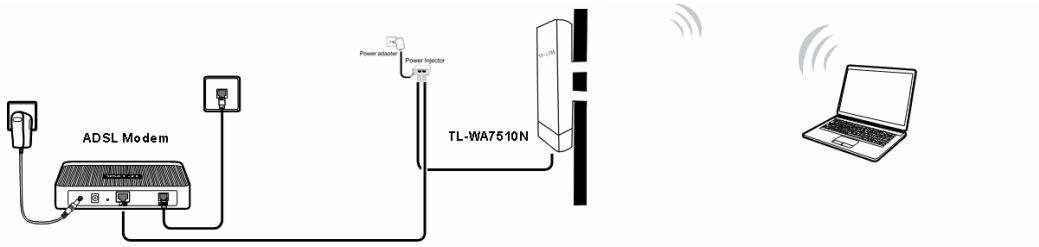


Figure 2-6 Hardware Installation of the TL-WA7510N in AP Router mode

1. Connect the LAN port of TL-WA7510N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the DSL/Cable Modem to the LAN port of the Power Injector with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
4. Power on the PC(s) and other connected devices (such as the ADSL modem).

Note:

In this mode, the LAN port of the Power Injector (connected to the LAN port of the Device) works as the WAN port.

2.3.3 AP Client Router Mode

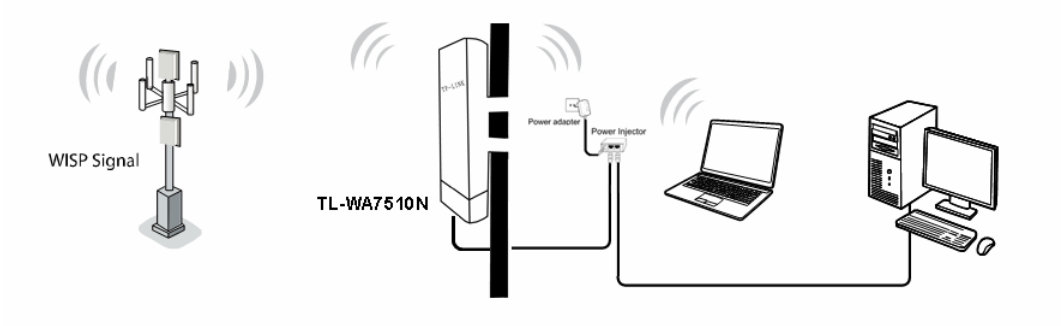


Figure 2-7 Hardware Installation of the TL-WA7510N in AP Client Router mode

1. Connect the LAN port of TL-WA7510N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the PC to the LAN port of the Power Injector with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
4. Power on the PC(s) and notebook(s).

Chapter 3 Quick Installation Guide

3.1 Configuring the PC

This chapter will guide you to configure your PC to communicate with the AP. The wireless adapter-equipped computers in your network must be in the same IP Address range without overlapping with each other. Manually configure the **IP address** as 192.168.1.* (* is any number within 1 to 253), and the **Subnet mask** as 255.255.255.0 for your PC following the instructions below.

Connect the local PCs to the LAN ports on the AP and configure the IP address manually for your PCs.

1. Click **Start** (in the lower left corner of the screen), right-click **My Network Connections** and choose **Properties**.

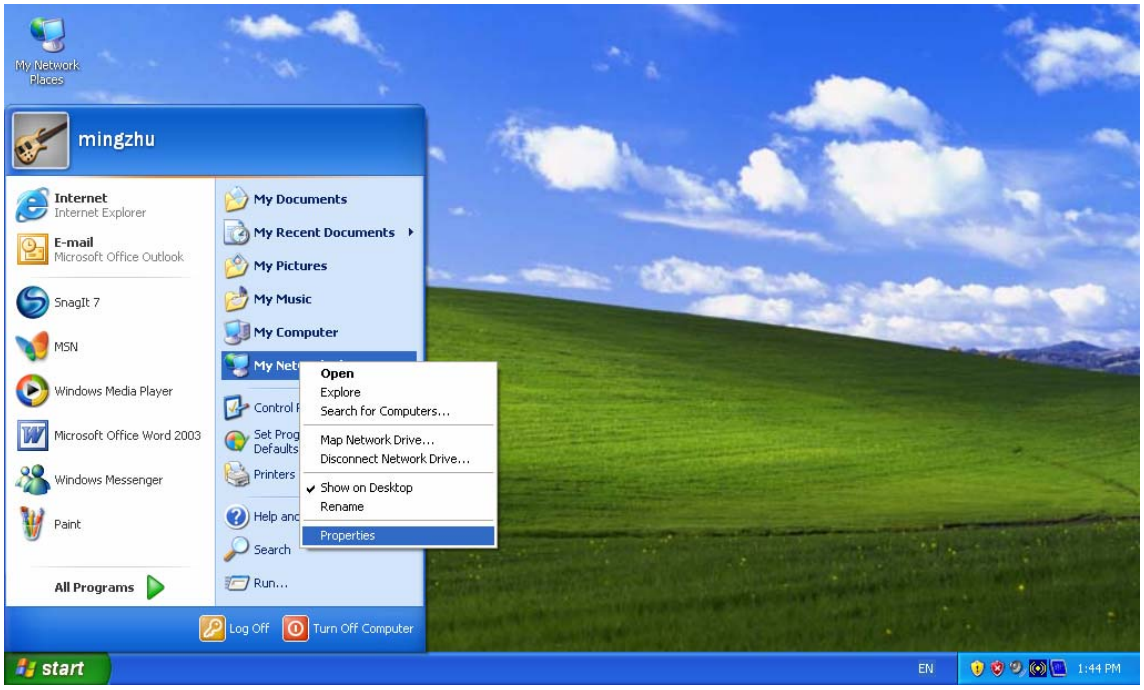


Figure 3-1

2. On the **My Network Connections** window shown as Figure 3-2 below, right-click **LAN (Local Area Connection)** and choose **Properties**.

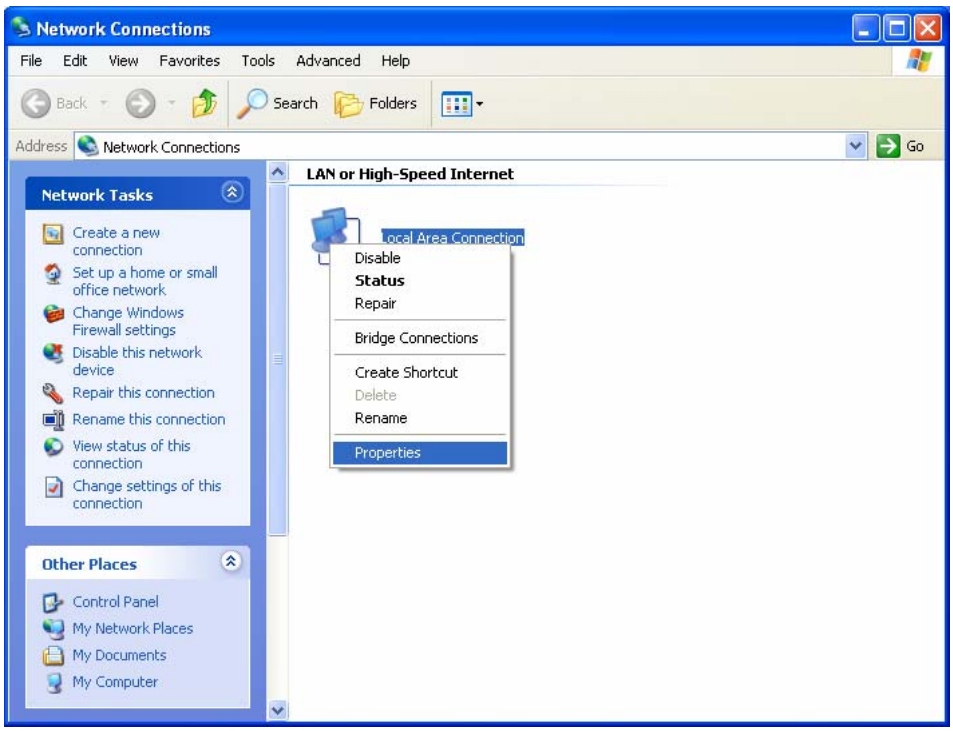


Figure 3-2

3. In the General tab of Internet Protocol (TCP/IP) Properties window, highlight Internet Protocol (TCP/IP) and click Properties.

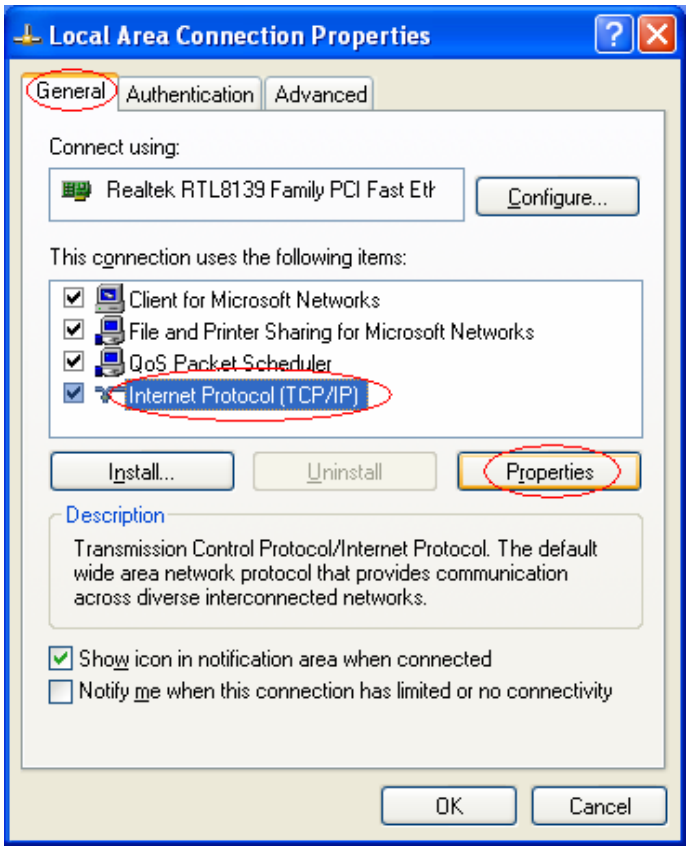


Figure 3-3

4. Configure the IP address manually.

 1) Select **Use the following IP address**.

 2) Enter 192.168.1.* (* is any integer between1 to 253) into the **IP address** filed, 255.255.255.0 into the **Subnet mask** filed.

 3) Click **OK** to keep your settings.

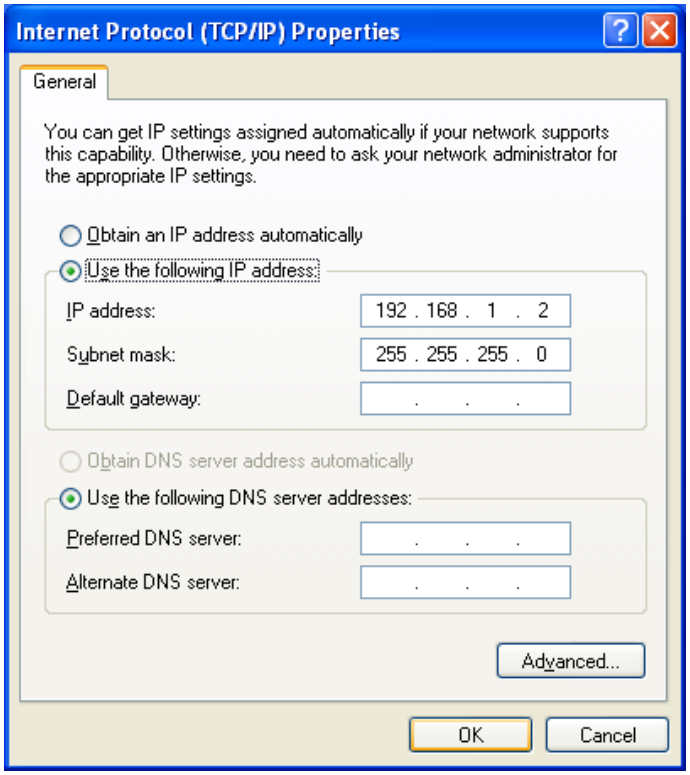


Figure 3-4

5. Verify the network connection between your PC and the AP via the Ping command. The following example is in Windows XP Operating System.

 1) Click **Start > Run** tab. Enter **cmd** in the filed and click **OK**.

 2) Type *ping 192.168.1.254* on the screen that displays and then press **Enter**.

 3) If the result displayed is similar to that shown in Figure 3-5 below, the connection between your PC and the AP has been successfully established.

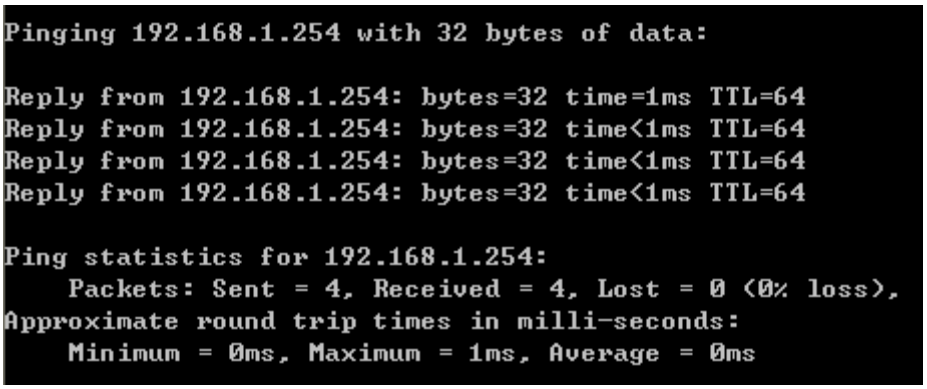


Figure 3-5

If the result displayed is similar to that shown in Figure 3-6 below, it means that your PC has not connected to the AP.

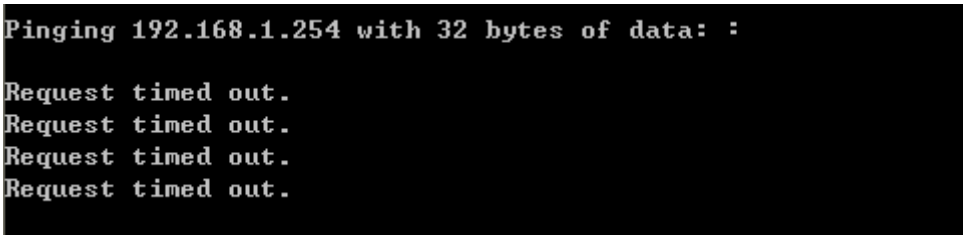


Figure 3-6

Please check following these steps:

a) Check to see if your PC and the AP are right connected. The LED of LAN port which you link to on the device and the LED on your PC's adapter should be lit up.

b) Make sure the TCP/IP for your PC is right configured. If the AP's IP address is 192.168.1.254, your PC's IP address must be within the range of 192.168.1.1 ~ 192.168.1.253.

3.2 Quick Setup

The TL-WA7510N is easy to configure and manage with. To access the configuration utility, open a web-browser and type in the default address http://192.168.1.254 in the address field of the browser.

1. Open your web browser. Type in the default address http://192.168.1.254 in the address field of web browser and then press **Enter**.



Figure 3-7 Login to the AP

Enter **admin** for the User Name and Password (both in lower case letters) in Figure 3-8 below. Then click **OK** or press Enter.

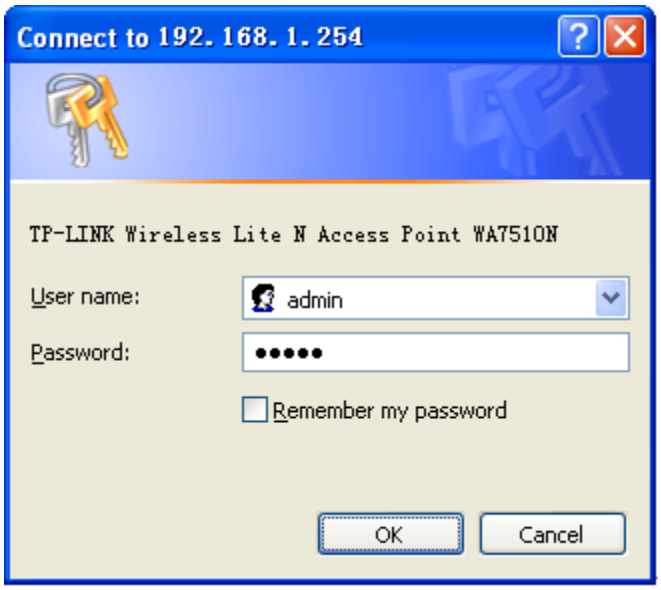


Figure 3-8 Login Windows

Note:

If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings**, in the screen that appears, cancel the **Using Proxy** checkbox, and click **OK** to finish it.

2. After a successful login, you can click the **Quick Setup** menu to quickly configure your Device.

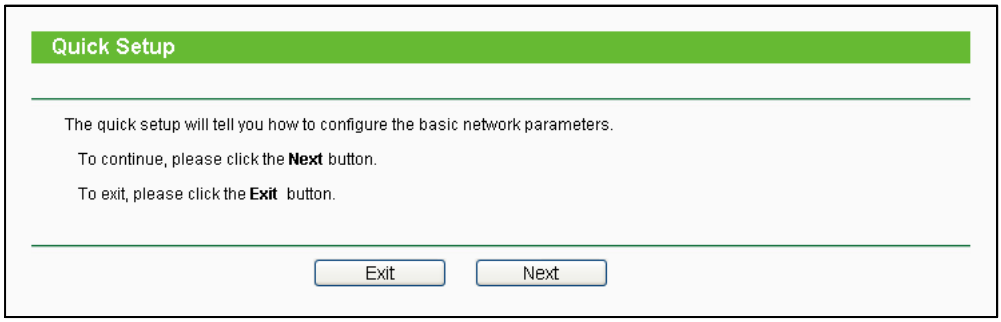


Figure 3-9 Quick Setup

3. Click **Next**, and then **Choose Operation mode** page will appear as shown in Figure 3-10 .

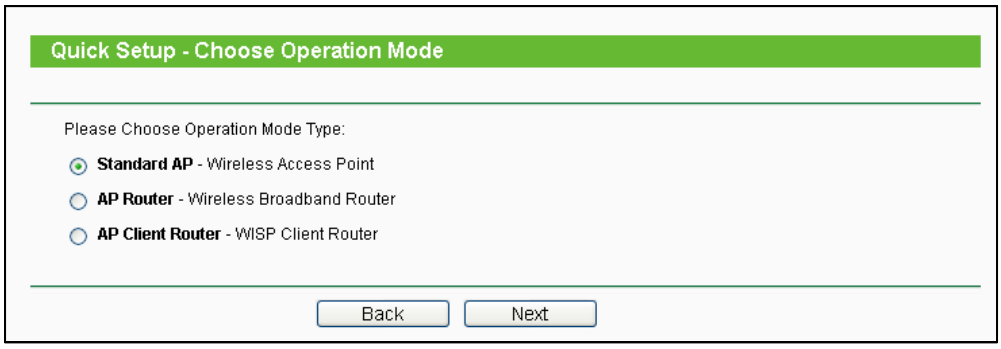


Figure 3-10 Choose Operation Mode

- **Standard AP**: In this mode, the device enables multi-users to access, and provides several wireless modes. such as AP, Client, Repeater and so on
- **AP Router**: In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while in AP Router mode.
- **AP Client Router**: In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port in AP Client Router mode. The Ethernet port acts as a LAN port.

3.2.1 Standard AP Mode

When you choose **Standard AP Mode** on **Operation Mode** page in Figure 3-10, take the following steps:

1. Click **Next** in Figure 3-10, and then **Wireless** page will appear as shown in Figure 3-11.



Figure 3-11

- **Operation Mode -** Several Operation Modes are supported, including: **Access Point, Multi-SSID, Client, Repeater, Universal Repeater, and Bridge with AP**. The available setting options are different in various operation modes.

1) **Access Point –** This operation mode allows wireless stations to access.



Figure 3-12

- **Wireless Radio**- Enable or disable the wireless radio.
- **SSID**- Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **TP-LINK _xxxxxx** (xxxxxx indicates the last unique six characters of each AP's MAC address), which can ensure your wireless network security. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySsid**.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.



Note Dialog

- **Channel**- This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the AP will select the best channel automatically.

- **Mode**- This field determines the wireless mode which the AP works on.
- **Max Tx Rate** - You can limit the maximum tx rate of the AP through this field.

You can select one of the following security options:

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.
 For **Hexadecimal**, the length should be between 8 and 64 characters.
 Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

2) Multi-SSID – AP can support up to 4 SSIDs.

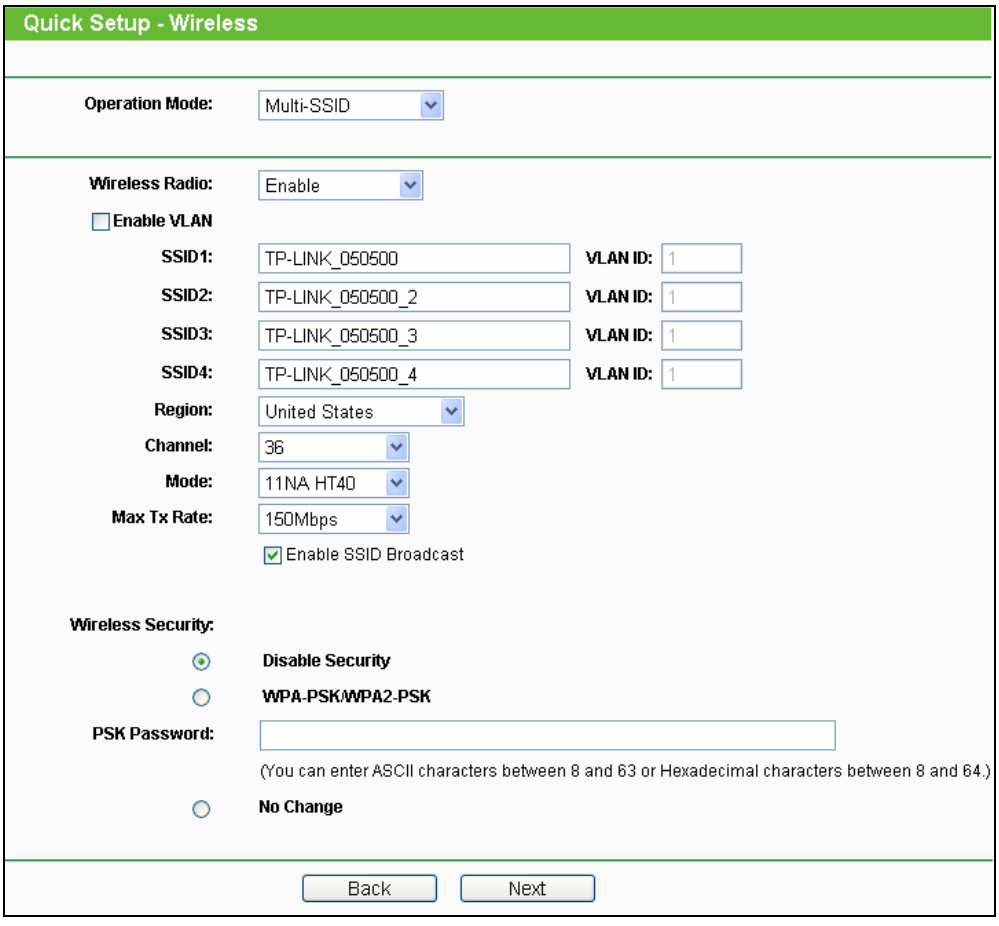


Figure 3-13

- **Wireless Radio**- The wireless radio of the AP can be enabled or disabled to allow or deny wireless stations to access. If enabled, the wireless stations will be able to access the AP; otherwise, wireless stations will not be able to access the AP.

- **Enable VLAN**- Check this box to enable the VLAN function. The AP supports up to 4 VLANs. All wireless PCs in the VLANs are able to access this AP. The AP can also work with an IEEE 802.1Q Tag VLAN supporting Switch. If this Switch enables the Tag VLAN function, besides all wireless PCs, only the PCs in the VLAN same with SSID1 are able to access the AP. If a PC is directly connected to the LAN port of the AP, please make sure that its adapter supports Tag function, or this PC will not be able to access the AP.
- **SSID**- Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. In Multi-SSID operation mode, enter SSID for each BSS in the field "SSID1" ~ "SSID4".
- **VLAN ID**- The ID of a VLAN. Only in the same VLAN can a wireless PC and a wired PC communicate with each other. The value can be between 1 and 4095. If the VLAN function is enabled, when AP forwards packets, the packets out from the LAN port will be added with an IEEE 802.1Q VLAN Tag, whose VLAN ID is just the ID of the VLAN where the sender belongs.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the AP in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.



Note Dialog

- **Channel**- This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode**-This field determines the wireless mode which the AP works on.
- **Max Tx Rate**- You can limit the maximum tx rate of the AP through this field.
- **Enable SSID Broadcast**- If you select the **Enable SSID Broadcast** checkbox, the AP will broadcast its name (SSID) on the air.

You can select one of the following security options:

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.

For **Hexadecimal**, the length should be between 8 and 64 characters.
Please note that the key is case sensitive.

- **Not Change**- If you chose this option, wireless security configuration will not change.

3) Client – The device will act as a wireless station to enable wired host(s) to access AP.

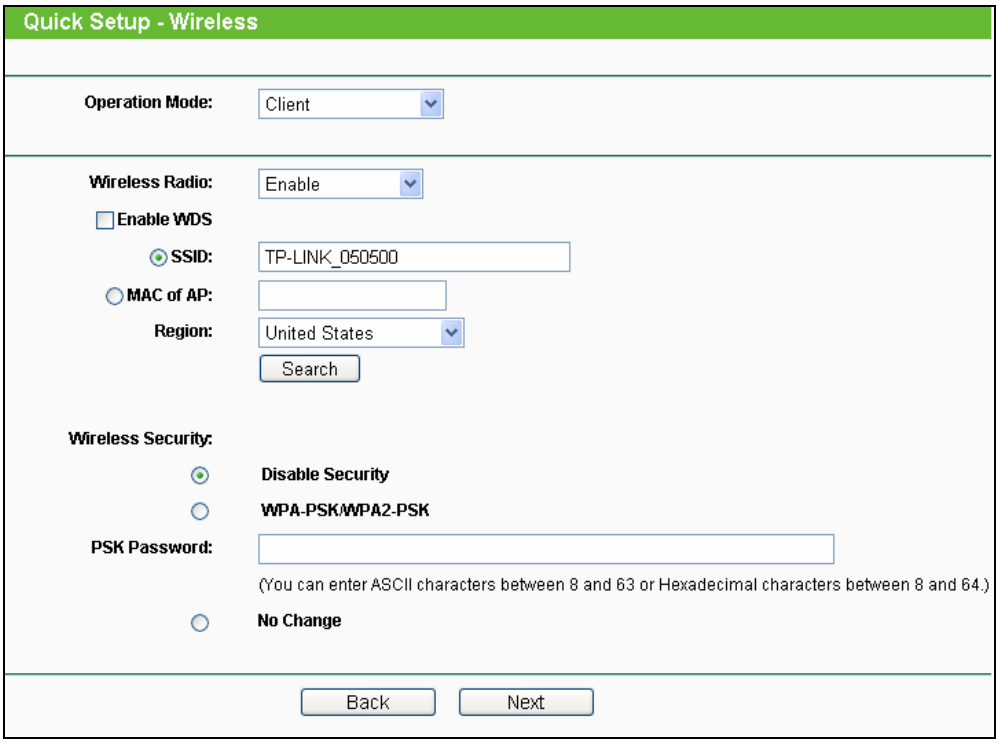


Figure 3-14

- **Wireless Radio**- The wireless radio of the AP can be enabled or disabled to allow or deny wireless stations to access. If enabled, the wireless stations will be able to access the AP; otherwise, wireless stations will not be able to access the AP.
- **Enable WDS-** The AP client can connect to AP with WDS enabled or disabled. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consisting of four address fields. If WDS is disabled, three address frames are used. If your AP supports WDS well, please enable this option.
- **SSID**- Enter the SSID of AP that you want to access. If you select the radio button before **SSID**, the AP client will connect to AP according to SSID.
- **MAC of AP**- Enter the MAC address of AP that you want to access. If you select the radio button before **MAC of AP**, the AP client will connect to AP according to MAC address.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the AP in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.



Note Dialog

You can select one of the following security options:

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.
 For **Hexadecimal**, the length should be between 8 and 64 characters.
 Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

4) Repeater

In Repeater mode, the AP with WDS enabled will relay data to an associated root AP. AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Please input the MAC address of root AP in the field "MAC of AP".

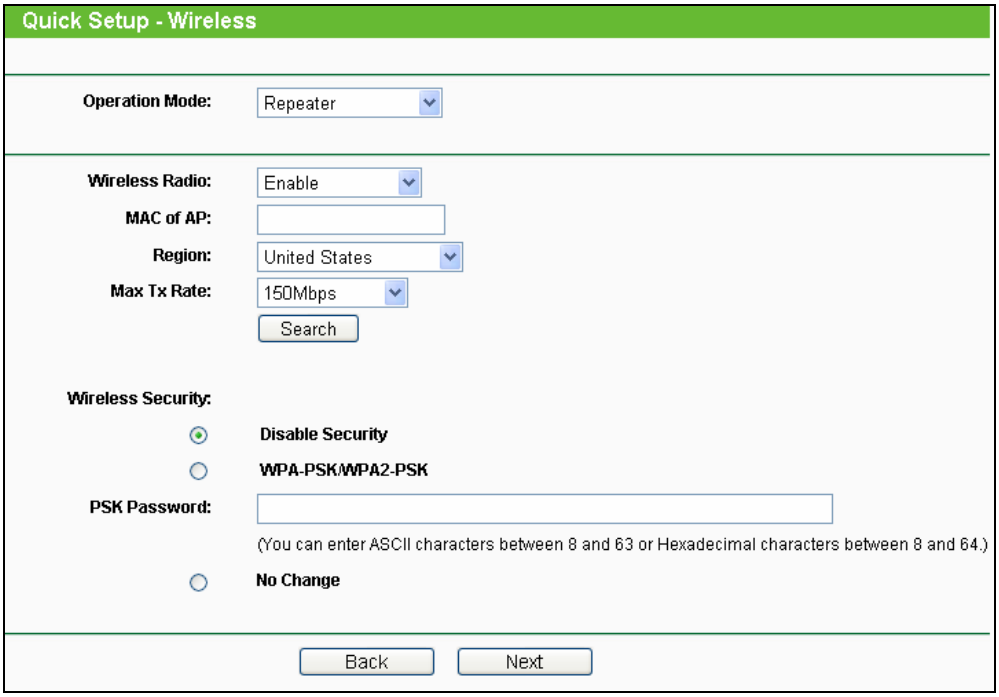


Figure 3-15

- **Wireless Radio**- The wireless radio of the AP can be enabled or disabled to allow or deny wireless stations to access. If enabled, the wireless stations will be able to access the AP; otherwise, wireless stations will not be able to access the AP.
- **MAC of AP**- Enter the MAC address of AP that you want to access. If you select the radio button before **MAC of AP**, the AP client will connect to AP according to MAC address.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the AP in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.



Note Dialog

- **Max Tx Rate**- You can limit the maximum tx rate of the AP through this field.

You can select one of the following security options:

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.
 For **Hexadecimal**, the length should be between 8 and 64 characters.
 Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

5) Universal Repeater

In Universal Repeater mode, the AP with WDS disabled will relay data to an associated root AP. AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Please input the MAC address of root AP in the field "MAC of AP".

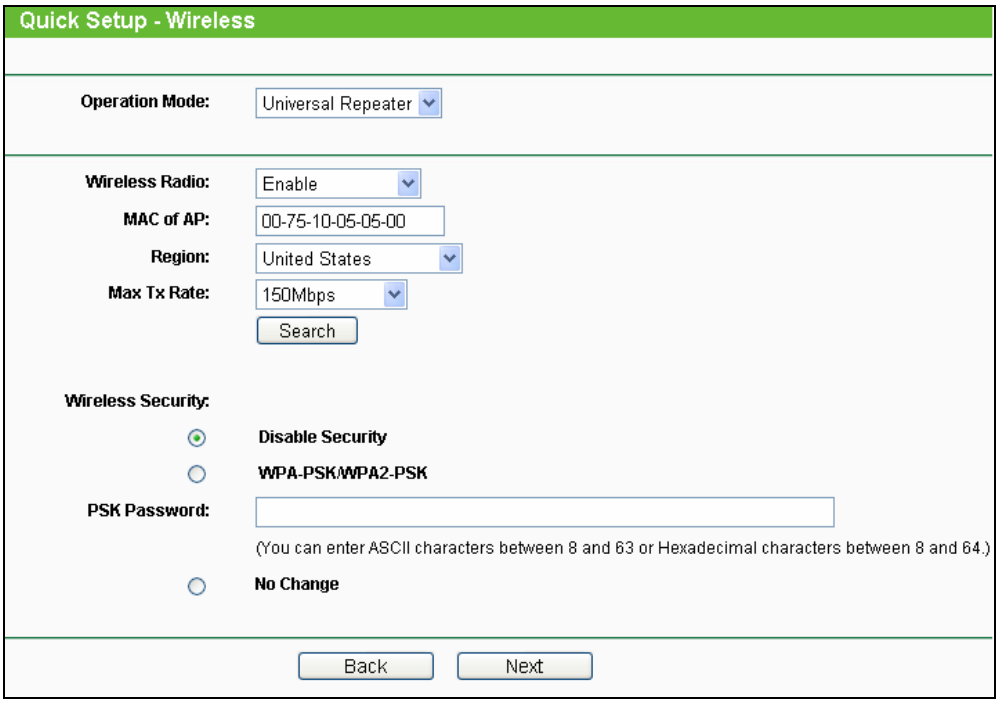


Figure 3-16

- **Wireless Radio**- The wireless radio of the AP can be enabled or disabled to allow or deny wireless stations to access. If enabled, the wireless stations will be able to access the AP; otherwise, wireless stations will not be able to access the AP.
- **MAC of AP**- Enter the MAC address of AP that you want to access. If you select the radio button before **MAC of AP**, the AP client will connect to AP according to MAC address.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the AP in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

 When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.



Note Dialog

- **Max Tx Rate**- You can limit the maximum tx rate of the AP through this field.

You can select one of the following security options:

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.

- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.
 For **Hexadecimal**, the length should be between 8 and 64 characters.
 Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

6) Bridge with AP

This operation mode bridges the AP and up to 4 APs also in bridge mode to connect two or more wired LANs. Please input the MAC address of other APs in the field "MAC of AP1" to "MAC of AP4". AP function will also start up.

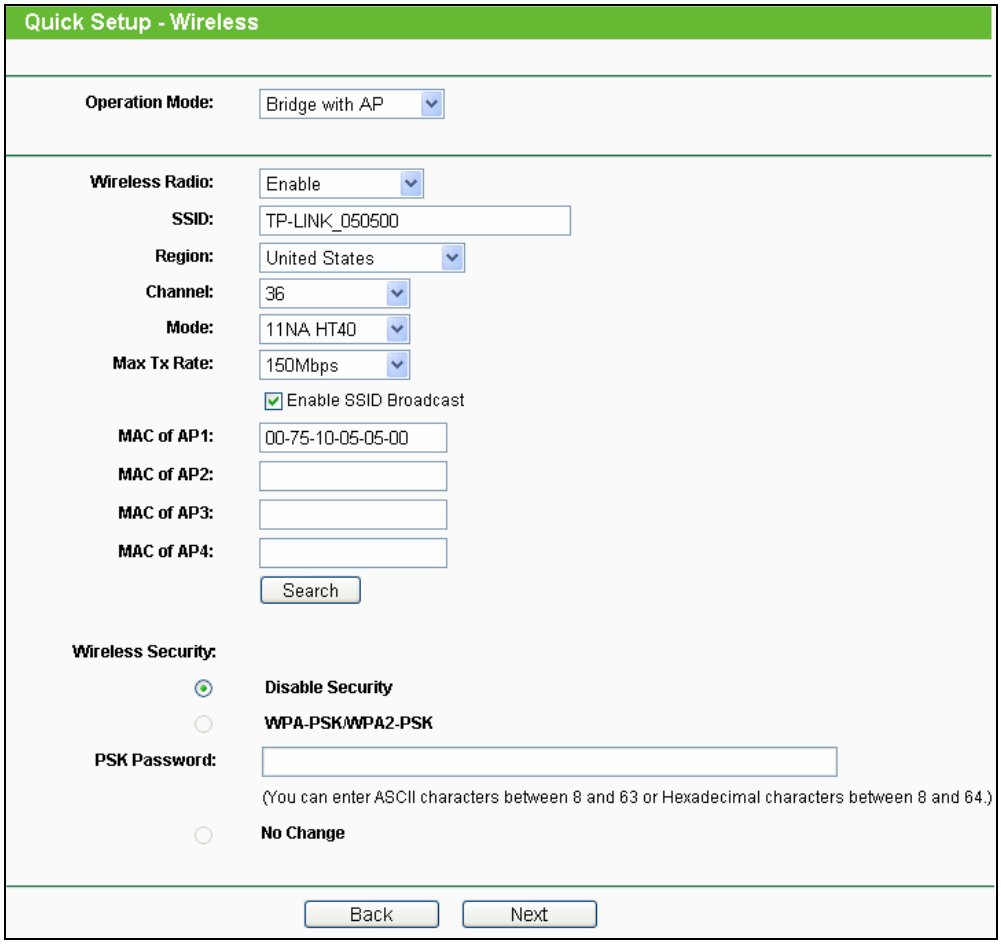


Figure 3-17

- **Wireless Radio**- The wireless radio of the AP can be enabled or disabled to allow or deny wireless stations to access. If enabled, the wireless stations will be able to access the AP; otherwise, wireless stations will not be able to access the AP.
- **SSID**- Enter the SSID of AP that you want to access. If you select the radio button before **SSID**, the AP client will connect to AP according to SSID.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the

AP in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

- When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.



Note Dialog

- **Channel**- This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode**-This field determines the wireless mode which the AP works on.
- **Max Tx Rate**- You can limit the maximum tx rate of the AP through this field.
- **Enable SSID Broadcast**- If you select the **Enable SSID Broadcast** checkbox, the AP will broadcast its name (SSID) on the air.
- **MAC of AP**- Enter the MAC address of AP that you want to access. If you select the radio button before **MAC of AP**, the AP client will connect to AP according to MAC address.

You can select one of the following security options:

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.
 For **Hexadecimal**, the length should be between 8 and 64 characters.
 Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

2. Click **Finish** button in Figure 3-18 to complete the **Quick Setup**.

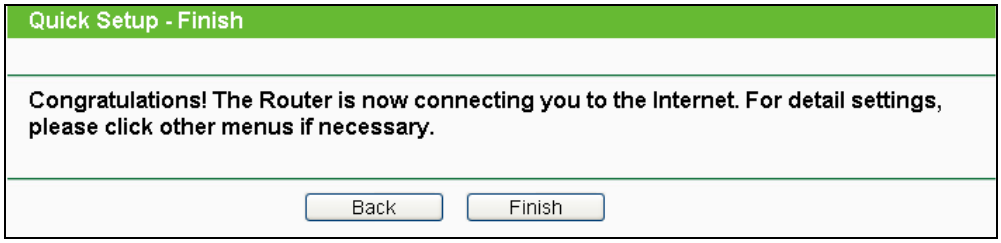


Figure 3-18

3.2.2 AP Router Mode

When you choose **AP Router Mode** on **Operation Mode** page in Figure 3-10, take the following steps:

1. Click **Next** in Figure 3-10, and then **WAN Connection Type** page will appear as shown in Figure 3-19.

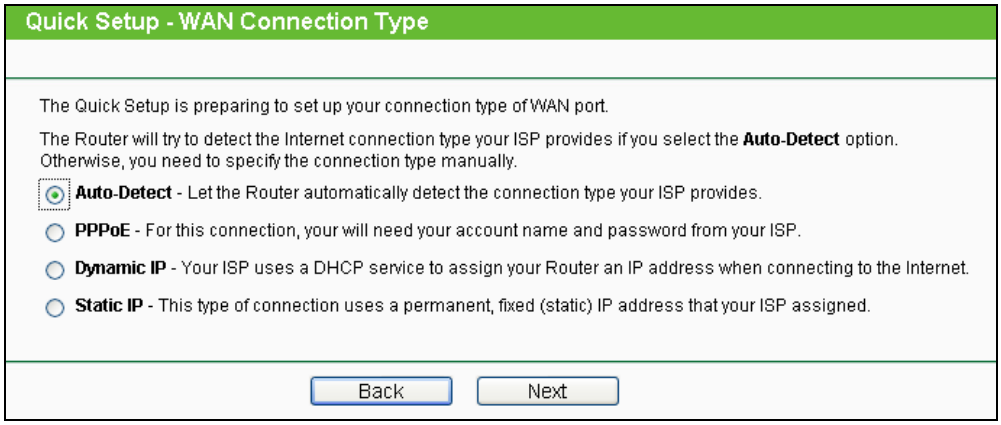


Figure 3-19

- **Auto Detect** - If you don't know the connection type your ISP provides, use this option to allow the Quick Setup to search your Internet connection for servers as well as protocols, and to determine your ISP configuration. Make sure the cable is securely plugged into the WAN port before detection. The appropriate configuration page will be displayed when an active Internet service is successfully detected by the Device.

 If you choose **Auto Detect** in Figure 3-19 and then click **Next**, Figure 3-20 will appear.

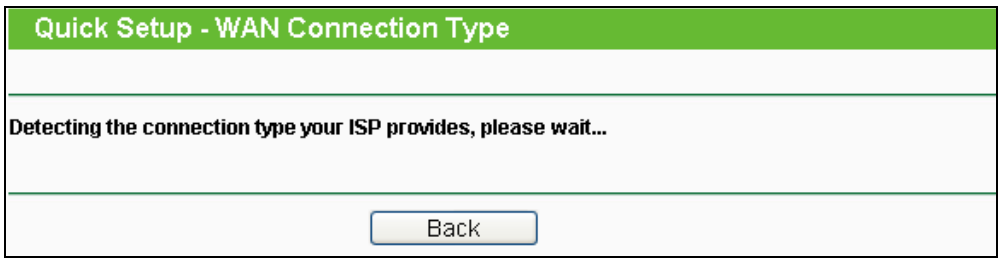


Figure 3-20

- **PPPoE** - If you have applied ADSL to realize Dial-up service, you should choose this type. In this condition, you should fill in both the User Name and Password that your ISP provides.

1) If you choose **PPPoE** in Figure 3-19 and then click **Next**, Figure 3-21 will appear.

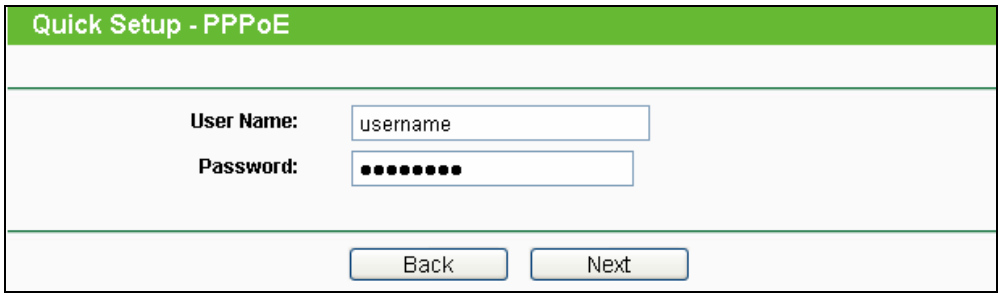


Figure 3-21

2) Enter the **User Name** and **Password** provided by your ISP and then click **Next**, Figure 3-22 will appear.

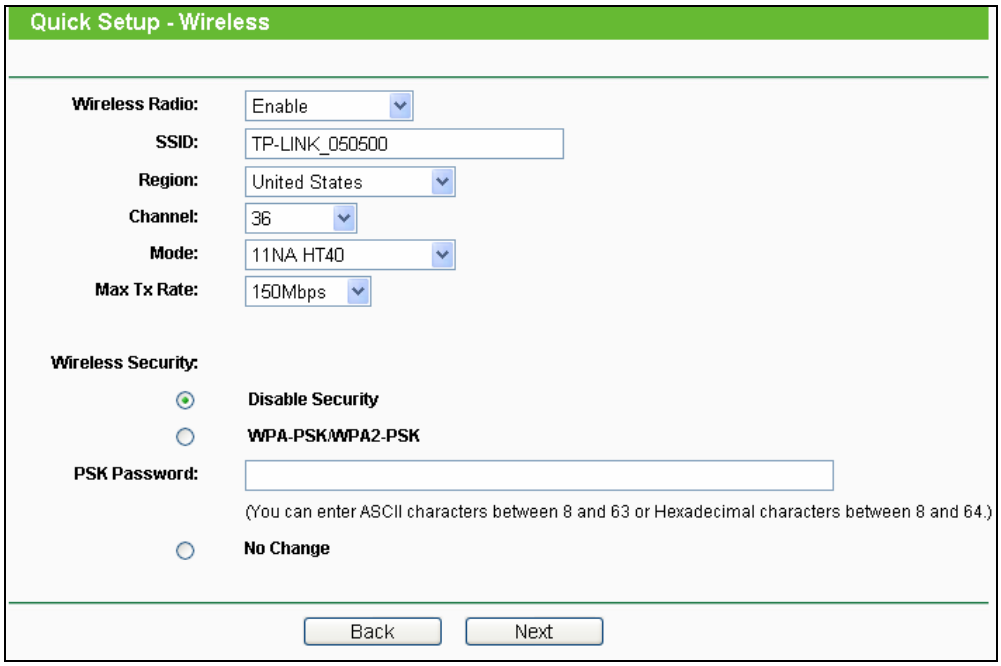


Figure 3-22

- **Wireless Radio**- Enable or disable the wireless radio.
- **SSID**- Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **TP-LINK_xxxxxx** (xxxxxx indicates the last unique six characters of each Device's MAC address), which can ensure your wireless network security. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySsid**.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- **Channel**- This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the Device will select the best channel automatically.

- **Mode**- This field determines the wireless mode which the Device works on.
- **Max Tx Rate**- You can limit the maximum tx rate of the Device through this field. You can select one of security options listed as the below items.
- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Device without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.
 For **Hexadecimal**, the length should be between 8 and 64 characters.
 Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

➢ **Dynamic IP**- When the Device connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type. The Device will get the IP address automatically from the DHCP server or the ISP if you choose the Dynamic IP type.

If you choose **Dynamic IP** in Figure 3-19 and then click **Next**, Figure 3-22 will appear.

➢ **Static IP** - In this type, you should manually fill in the **IP address**, **Subnet Mask**, **Default Gateway**, and **DNS** IP address, which are specified by your ISP.

1) If you choose **Static IP** in Figure 3-19 and then click **Next**, Figure 3-23 will appear.

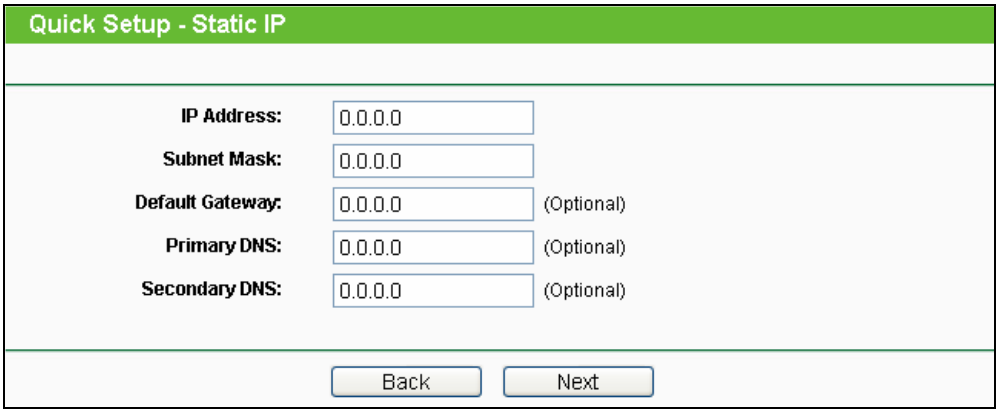


Figure 3-23

- **IP Address**- This is WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address in the field.
- **Subnet Mask**- It is used for the WAN IP address, which is usually 255.255.255.0.
- **Default Gateway**- Enter the default gateway in the blank if required.
- **Primary DNS**- Enter the DNS IP address in the blank if required.
- **Secondary DNS**- If your ISP provides another DNS IP address, enter it in this field.

☞ **Note:**

The IP parameters should have been provided by your ISP.

2) After you have entered the above necessary parameters and then click **Next**, Figure 3-22 will then appear.

2. When you finish the wireless setting in Figure 3-22 and click **Next**, then Figure 3-24will appear, where you can click **Finish** button to complete the **Quick Setup**.

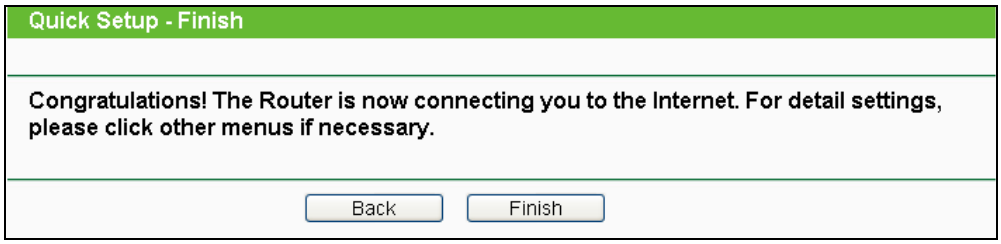


Figure 3-24

3.2.3 AP Client Router Mode

When you choose **AP Client Router Mode** on **Operation Mode** page in Figure 3-10 , take the following steps:

1. Click **Next** in Figure 3-10, and then **WAN Connection Type** page will appear as shown in Figure 3-25.

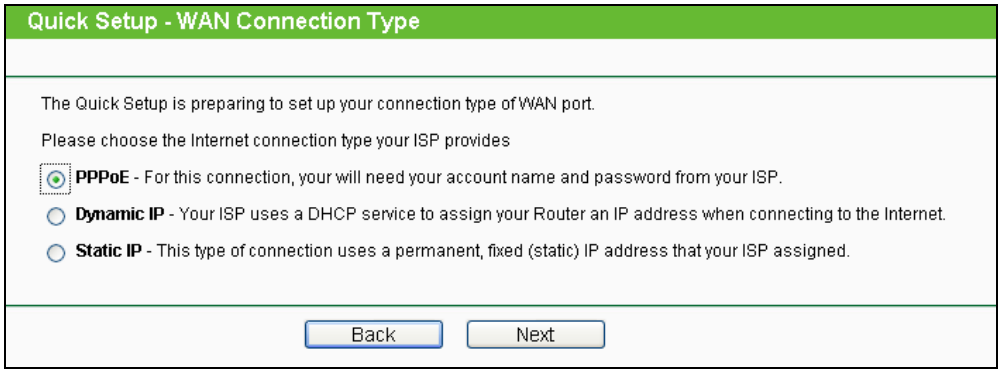


Figure 3-25

- **PPPoE** - If you have applied ADSL to realize Dial-up service, you should choose this type. In this condition, you should fill in both the User Name and Password that your ISP supplies.

 1) If you choose **PPPoE** in Figure 3-25 and then click **Next**, Figure 3-26 will appear.

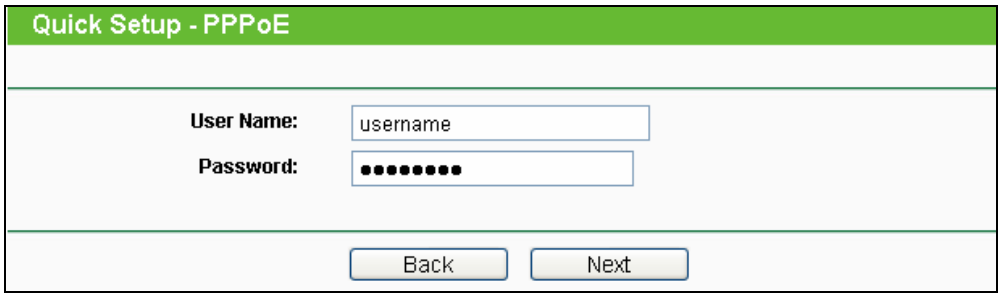


Figure 3-26

2) Enter the **User Name** and **Password** provided by your ISP, then click **Next**, Figure 3-27 will appear.

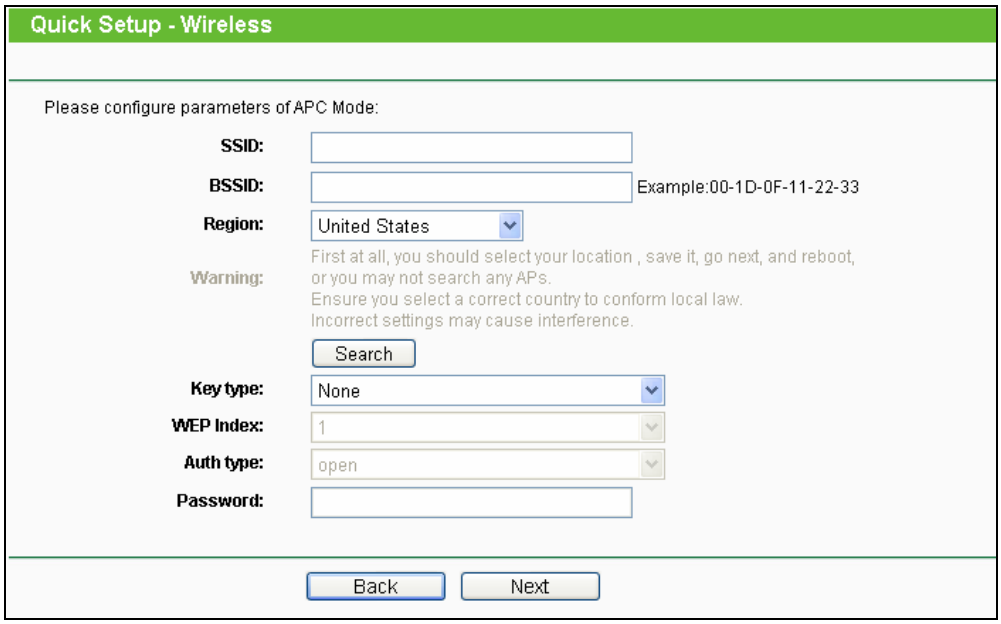


Figure 3-27

- **SSID -** The SSID of the AP your Device is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID -** The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- **Search -** Click this button, you can search the AP which runs in the current channel.
- **Key type -** This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- **WEP Index -** This option should be chosen if the key type is WEP (ASCII) or WEP (HEX).It indicates the index of the WEP key.
- **Auth Type -** This option should be chosen if the key type is WEP (ASCII) or WEP (HEX).It indicates the authorization type of the Root AP.

- **Password -** If the AP your Device is going to connect needs password, you need to fill the password in this blank.

➢ **Dynamic IP**- When the Device connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type. The Device will get the IP address automatically from the DHCP server or the WISP if you choose the Dynamic IP type.

If you choose **Dynamic IP** in Figure 3-25 and then click **Next**, the wireless setting page as in Figure 3-27 will appear.

➢ **Static IP** - In this type, you should manually fill in the **IP address**, **Subnet Mask**, **Default Gateway**, and **DNS** IP address, which are specified by your ISP.

1) If you choose **Static IP** in Figure 3-25 and then click **Next**, Figure 3-28 will appear.

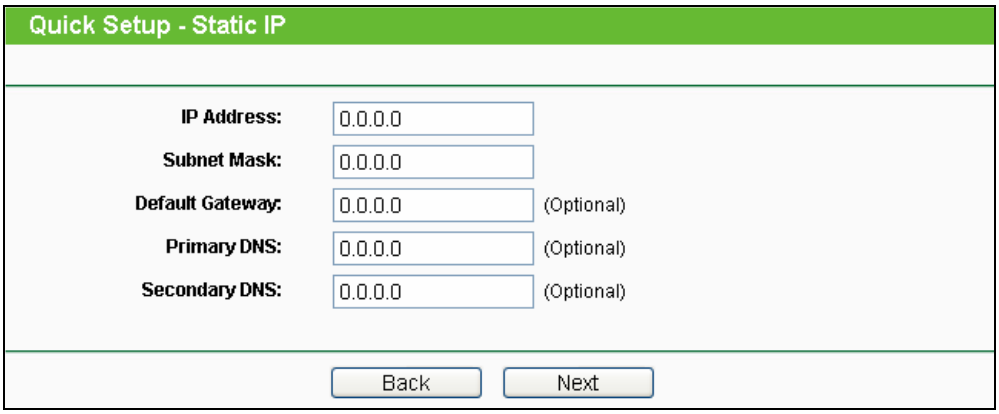


Figure 3-28

- **IP Address**- This is WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask**- It is used for the WAN IP address, which is usually 255.255.255.0.
- **Default Gateway**- Enter the default gateway in the blank if required.
- **Primary DNS**- Enter the DNS IP address in the blank if required.
- **Secondary DNS**- If your WISP provides another DNS IP address, enter it in this field.

☞ **Note:**

The IP parameters should have been provided by your WISP.

2) After you have entered the above necessary parameters and then click **Next**, the wireless setting page as in Figure 3-27 will then appear.

2. When you finish the wireless setting in Figure 3-27 and click **Next**, then Figure 3-29 will appear, where you can click **Finish** button to complete the **Quick Setup**.

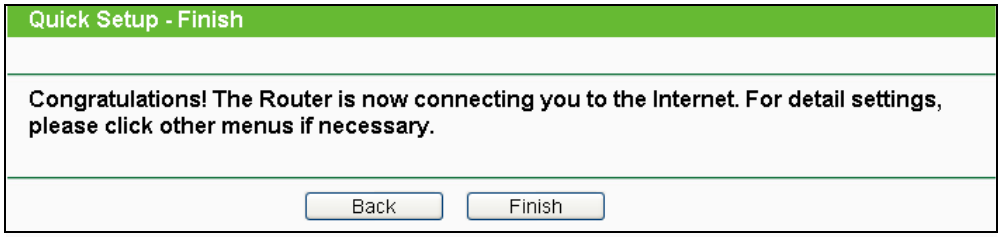


Figure 3-29

Chapter 4 Configuring Standard AP Mode

This chapter will show each Web page's key functions and the configuration way under Standard AP Mode.

4.1 Login

Open your web browser. Type in the default address http://192.168.1.254 in the address field of web browser and then press **Enter**.



Figure 4-1 Login to the AP

Enter **admin** for the User Name and Password (both in lower case letters) in Figure 4-2 below. Then click **OK** or press Enter.

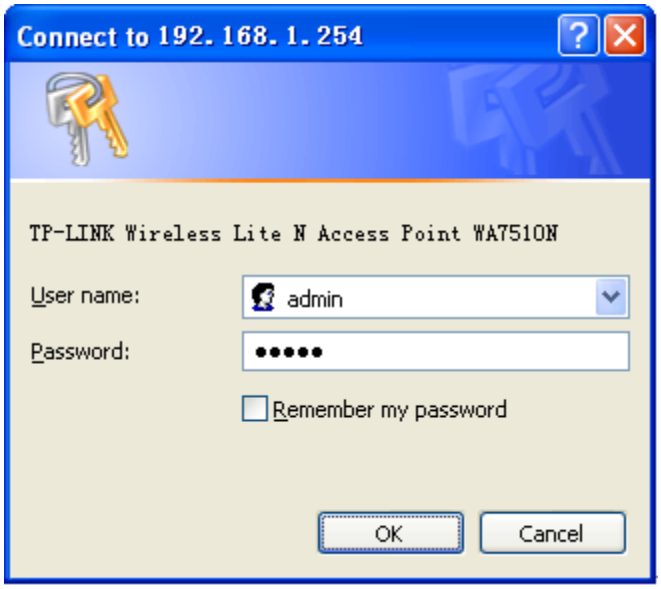


Figure 4-2 Login Windows

Note:

If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings**, in the screen that appears, cancel the **Using Proxy** checkbox, and click **OK** to finish it.

After a successful login, you can configure and manage the Device. There are eight main menus on the leftmost column of the web-based management page as in Figure 4-3: **Status**, **Quick Setup**, **QSS**, **Operation Mode**, **Network**, **Wireless**, **DHCP** and **System Tools**. Sub-menus will be available after clicking one of the main menus. On the right of the web-based management page lays the detailed explanations and instructions for the corresponding page.

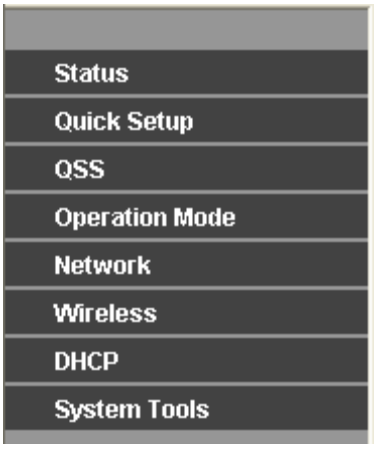


Figure 4-3 the main menu

4.2 Status

Selecting **Status** will enable you to view the AP's current status and configuration, all of which are read-only.

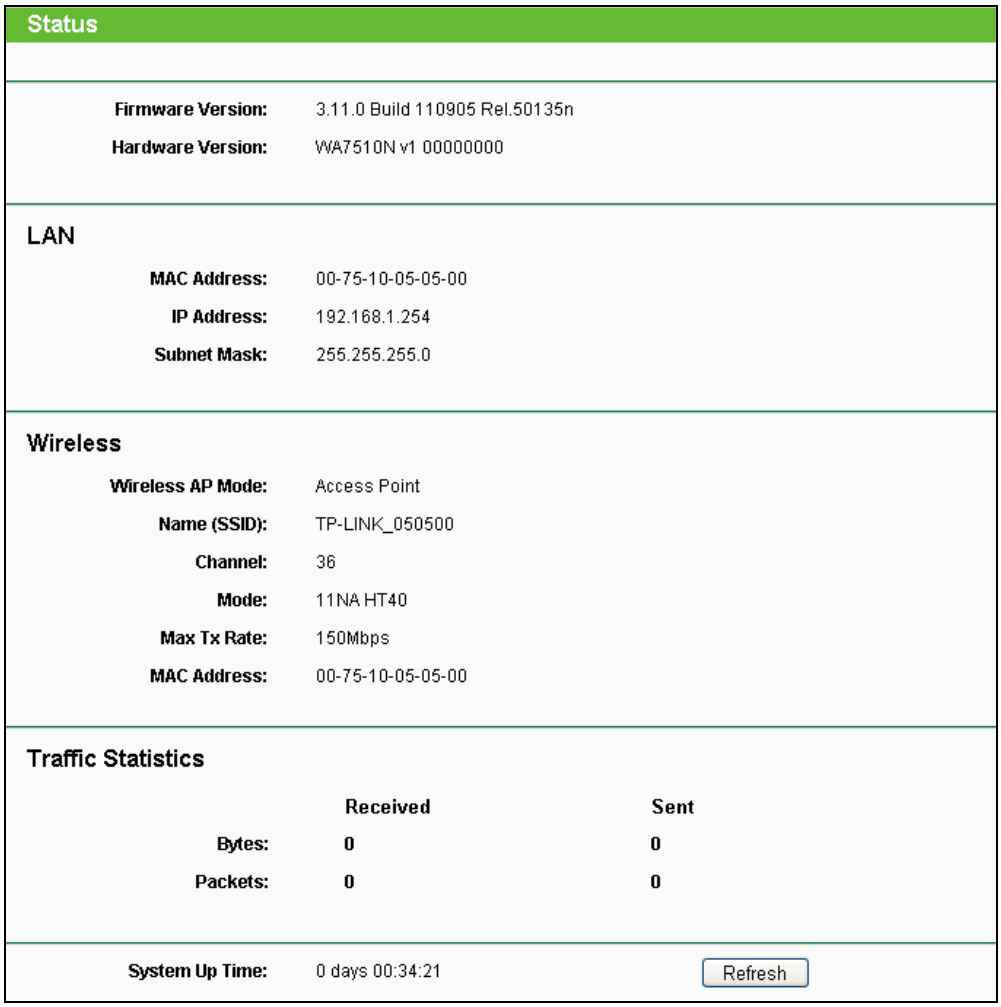


Figure 4-4 Status

- **Firmware Version -** The current firmware version of the AP.
- **Hardware Version -** The current hardware version of the AP.
- **LAN -** The following is the information of wired LAN. You can configure them in the **Network** page.
 - **MAC Address -** The physical address of the system, as seen from the LAN.
 - **IP Address -** The IP address of the wired LAN.
 - **Subnet Mask -** The subnet mask associated with IP address.
- **Wireless** - These are the current settings or information for wireless. You can configure them in the **Wireless -> Wireless Settings** page.
 - **Wireless AP Mode -** The current wireless AP mode which the AP works on.
 - **Name (SSID) -** The SSID of the AP.
 - **Channel -** The current wireless channel in use.
 - **Mode -** The current wireless mode which the AP works on.
 - **Max Tx Rate -** The maximum tx rate.
 - **MAC Address -** The physical address of the AP, as seen from the WLAN.
- **Traffic Statistics** - The system traffic statistics.
 - **Sent (Bytes) -** Traffic that counted in bytes has been sent out from WLAN.
 - **Sent (Packets) -** Traffic that counted in packets has been sent out from WLAN.
 - **Received (Bytes) -** Traffic that counted in bytes has been received from WLAN.
 - **Received (Packets) -** Traffic that counted in packets has been received from WLAN.
- **System Up Time** - The length of the time since the AP was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the AP.

4.3 Quick Setup

Please refer to Section 3.2 Quick Setup – 3.2.1 Standard AP Mode for more details.

4.4 QSS

QSS (**Quick Secure Setup**) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to an existing network quickly by function.

☞ **Note:**

The **QSS** function is only available when the Operation Mode is set to Access Point and Multi-SSID. Here we take the Access Point mode for example.

Select menu **QSS**, you will see the next screen as shown in Figure 4-5.

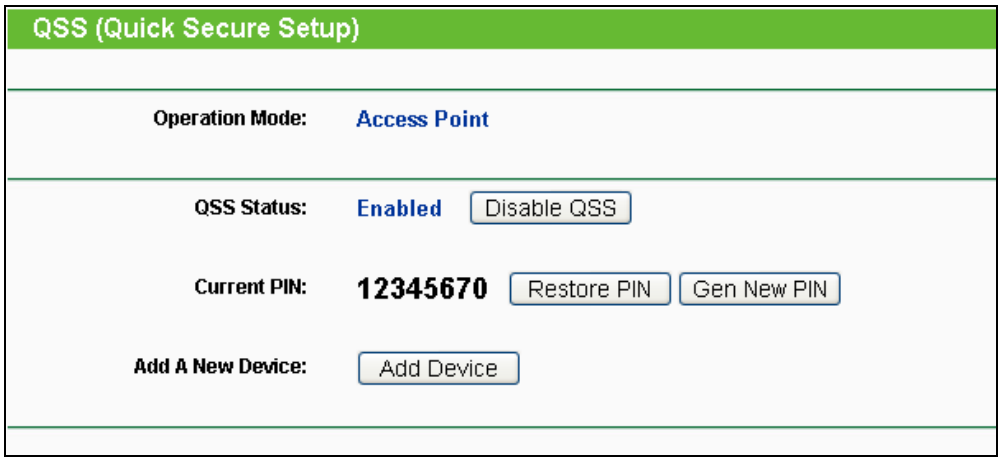


Figure 4-5 QSS

- **QSS Status** - Enable or disable the QSS function here.
- **Current PIN** - The current value of the Device's PIN displayed here. The default PIN of the Device can be found in the label or User Guide.
- **Restore PIN** - Restore the PIN of the Device to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the Device's PIN. You can ensure the network security by generating a new PIN.
- **Add A New Device** - You can add the new device to the existing network manually by clicking **Add Device** button.

☞ **Note:**

The **QSS** function cannot be configured if the Wireless Function of the Device is disabled. Please make sure the Wireless Function is enabled before configuring the **QSS.**

- **To add a new device:**

1. If the new device supports Wi-Fi Protected Setup and is equipped with a configuration button, you can add it to the network by pressing the configuration button on the device.
2. If the new device supports Wi-Fi Protected Setup and the connection way using PIN, you can add it to the network by entering the Device's PIN.

☞ **Note:**

To build a successful connection by QSS, you should also do the corresponding configuration on a wireless adapter for QSS function meanwhile.

For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 4-5, and then the following screen will appear.

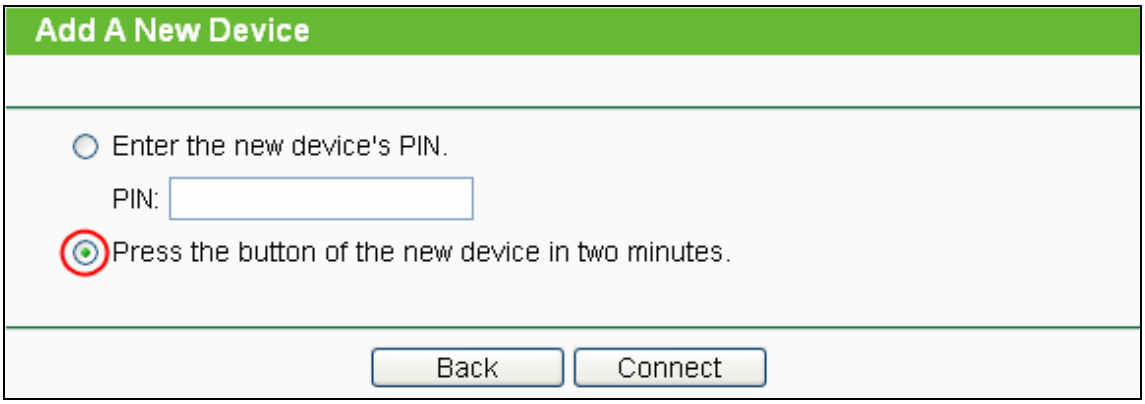


Figure 4-6 Add A New Device

Step 2: Choose "**Press the button of the new device in two minutes**" and click **Connect**.

Step 3: Configure the wireless adapter for QSS function by choosing "**Push the button on my access point**" in the QSS configuration utility as below, and then click **Next**.

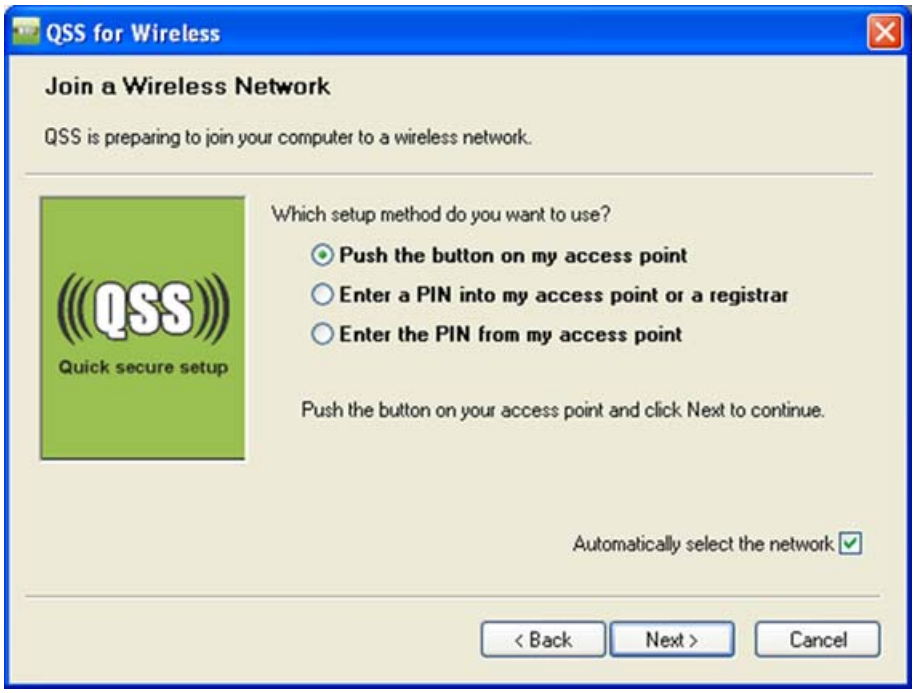


Figure 4-7 The QSS Configuration Screen of Wireless Adapter

Step 4: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.

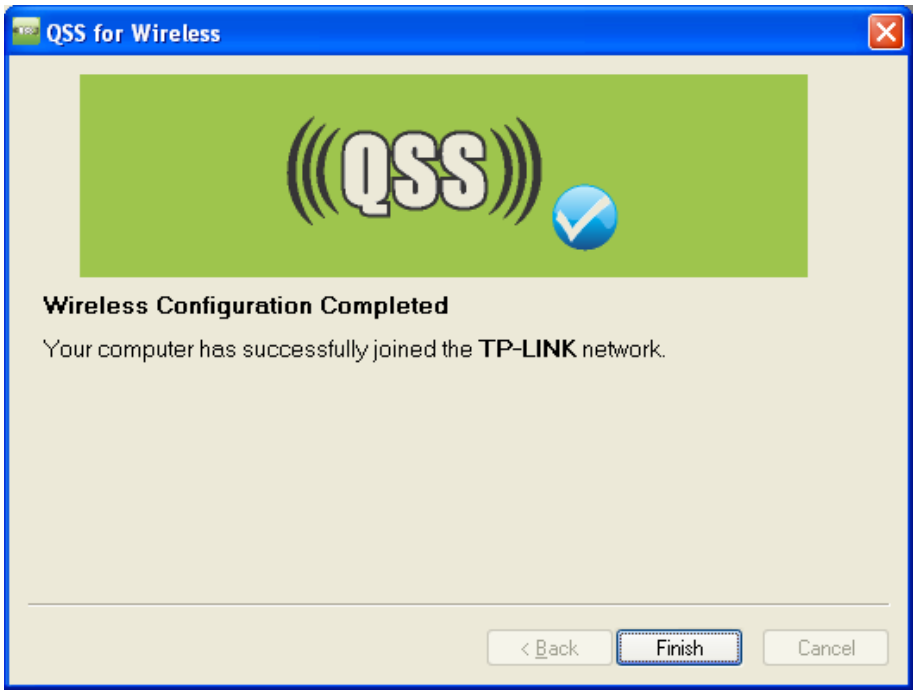


Figure 4-8 The QSS Configuration Screen of Wireless Adapter

II. By PIN

If the device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN in the following two methods.

Method One: Enter the PIN into my AP

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 4-5, and then the following screen will appear.

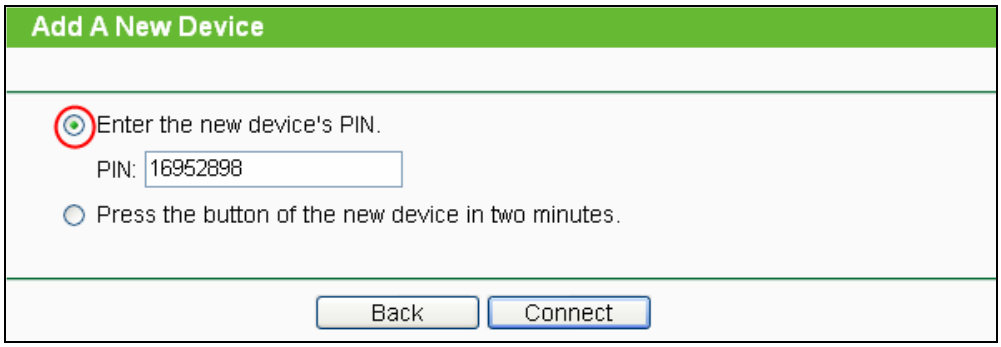


Figure 4-9 Add A New Device

Step 2: Choose "**Enter the new device's PIN**" and enter the PIN code（take 16952898 for example）of the wireless adapter in the field after **PIN** as shown in the figure above. Then click **Connect.**

☞ **Note:**

The PIN code of the adapter is always displayed on the QSS configuration screen as shown in Figure 4-10.

Step 3: Configure the wireless adapter for QSS function by choosing "**Enter a PIN into my access point or a registrar**" in the configuration utility of the QSS as below, and click **Next**.

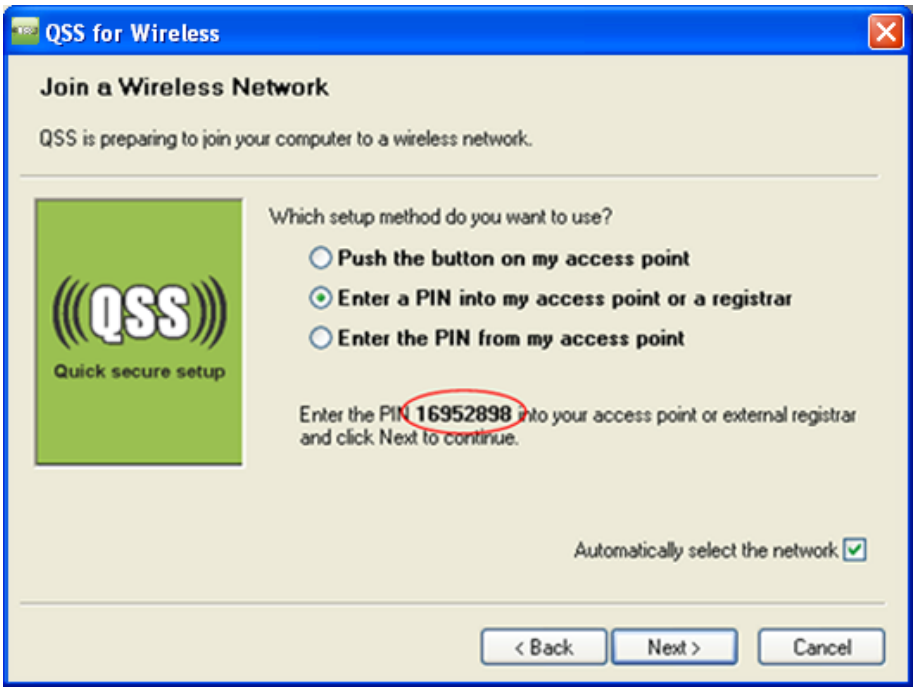


Figure 4-10 The QSS Configuration Screen of Wireless Adapter

☞ **Note:**

In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

Method Two: Enter the PIN from my AP

Step 1: Get the Current PIN code of the AP in Figure 4-11(Each AP has its unique PIN code. Here takes the default PIN code 12345670 of this AP for example).

Step 2: Configure the wireless adapter for QSS function by choosing "**Enter a PIN from my access point**" in the configuration utility of the QSS as below, and enter the PIN code of the AP into the field after "**Access Point PIN**". Then click **Next**.

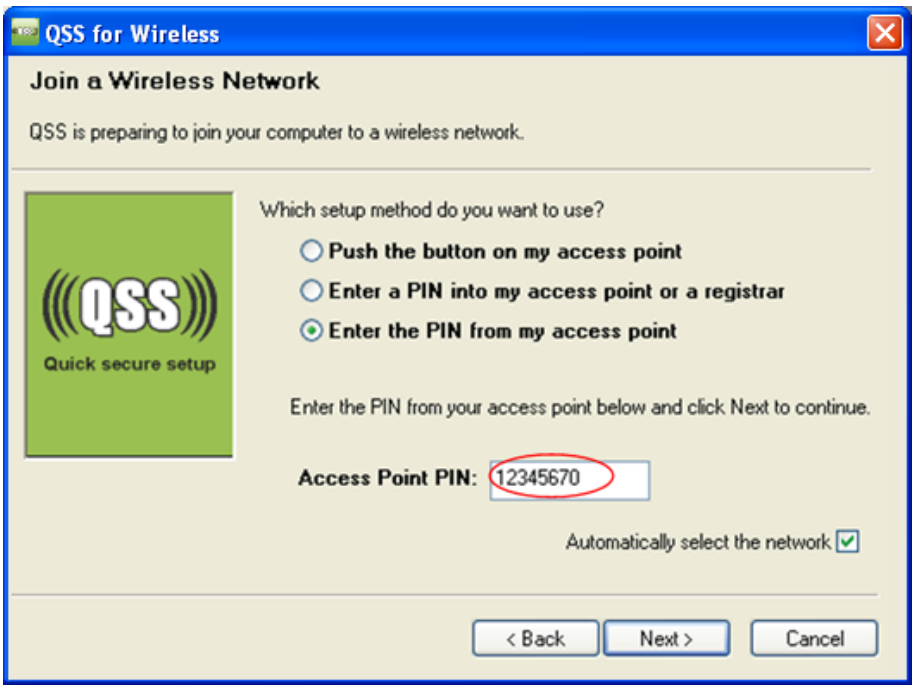


Figure 4-11 The QSS Configuration Screen of Wireless Adapter

Note:

The default PIN code of the AP can be found in its label or the QSS configuration screen as in Figure 4-5.

You will see the following screen when the new device has successfully connected to the network.

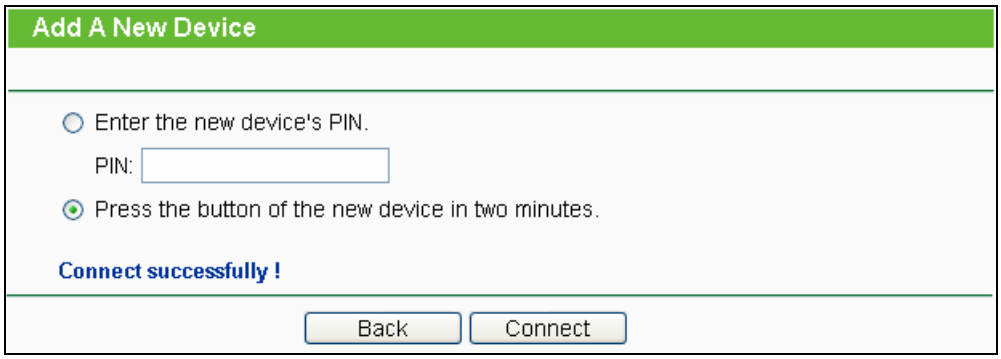


Figure 4-12

Note:

The QSS function cannot be configured if the Wireless function of the AP is disabled. Please make sure the Wireless function is enabled before configuring the QSS.

4.5 Operation Mode

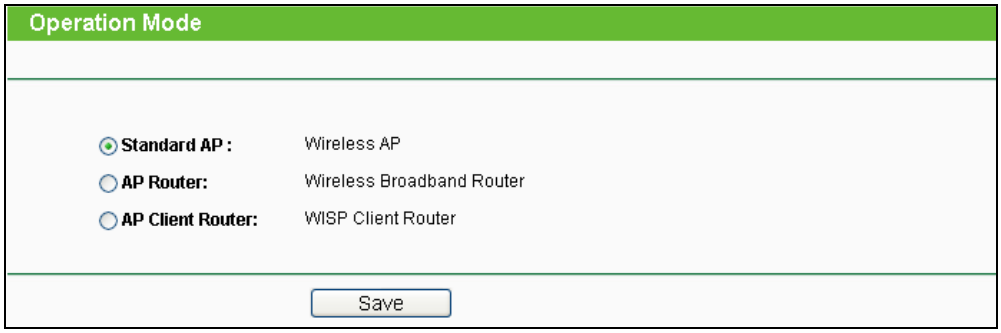


Figure 4-13

- **Standard AP**: In this mode, the device enables multi-users to access, and provides several wireless modes, such as AP, Client, Repeater and so on.
- **AP Router**: In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.
- **AP Client Router**: In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at AP Client Router mode. The Ethernet port acts as a LAN port.

Be sure to click the **Save** button to save your settings on this page.

Note:

The Device will reboot automatically after you click the **Save** button.

4.6 Network

The **Network** option allows you to customize your local network manually by changing the default settings of the AP.



Figure 4-14 The Network menu

Selecting **Network > LAN** will enable you to configure the IP parameters of LAN on the following page.

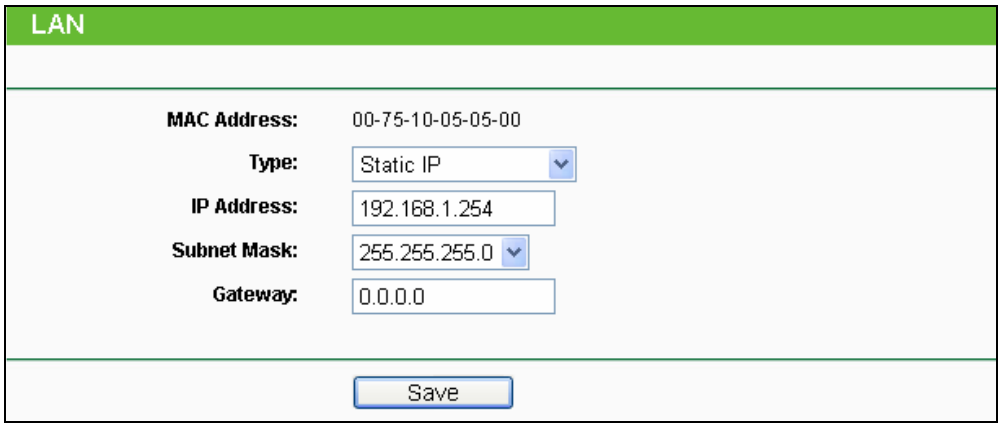


Figure 4-15 LAN

- **MAC Address**- The physical address of the LAN ports, as seen from the LAN. The value can not be changed.
- **Type**- Choosing dynamic IP to get IP address from DHCP server, or choosing static IP to configure IP address manually.
- **IP Address**- Enter the IP address of your system in dotted-decimal notation (factory default: 192.168.1.254).
- **Subnet Mask**- It is an address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.
- **Gateway**- The gateway should be in the same subnet as your IP address.

Note:

1. If you change the IP address, you must use the new IP address to login the system.
2. If you select the type of dynamic IP, the DHCP server in this device will not start up.
3. If the new IP address you set is not in the same subnet, the IP Address pool in the DHCP server will not take effect, until they are re-configured.
4. The device will reboot automatically after you click the **Save** button.

Click the **Save** button to save your settings.

Note:

When you choose the Dynamic IP mode, the DHCP Server function will be disabled.

4.7 Wireless

The **Wireless** option improves functionality and performance for wireless network. It can help you make the AP an ideal solution for your wireless network. There are eight submenus under the Wireless menu (shown in Figure 4-16): **Wireless Settings**, **Wireless Security**, **Wireless MAC**

Filtering, **Wireless Advanced**, **Antenna Alignment, Distance Settings, Throughput Monitor** and **Wireless Statistics**.

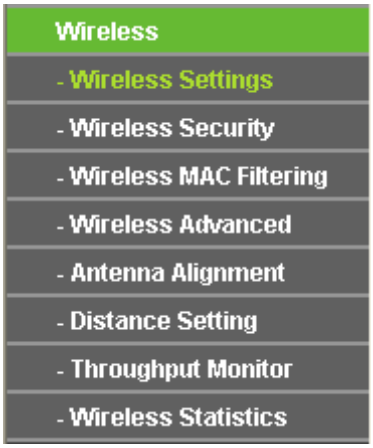


Figure 4-16 Wireless menu

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.7.1 Wireless Settings

Selecting **Wireless > Wireless Settings** will enable you to configure the basic settings for your wireless network. The setting page allows you to configure the wireless mode for your device. Six operation modes are supported here, including Access Point, Multi-SSID, Client, Repeater, Universal Repeater and Bridge with AP.

Please refer to Section 3.2 Quick Setup – 3.2.1 Standard AP Mode for more details.

4.7.2 Wireless Security

Selecting **Wireless > Wireless Security** will enable you to configure wireless security for your wireless network to protect your data from intruders. The AP provides three security types: WEP, WPA/WPA2 and WPA-PSK/WPA2-PSK. Wireless security can be set on the following screen shown as Figure 4-17. The security options are different for different operation mode.

1) Access Point

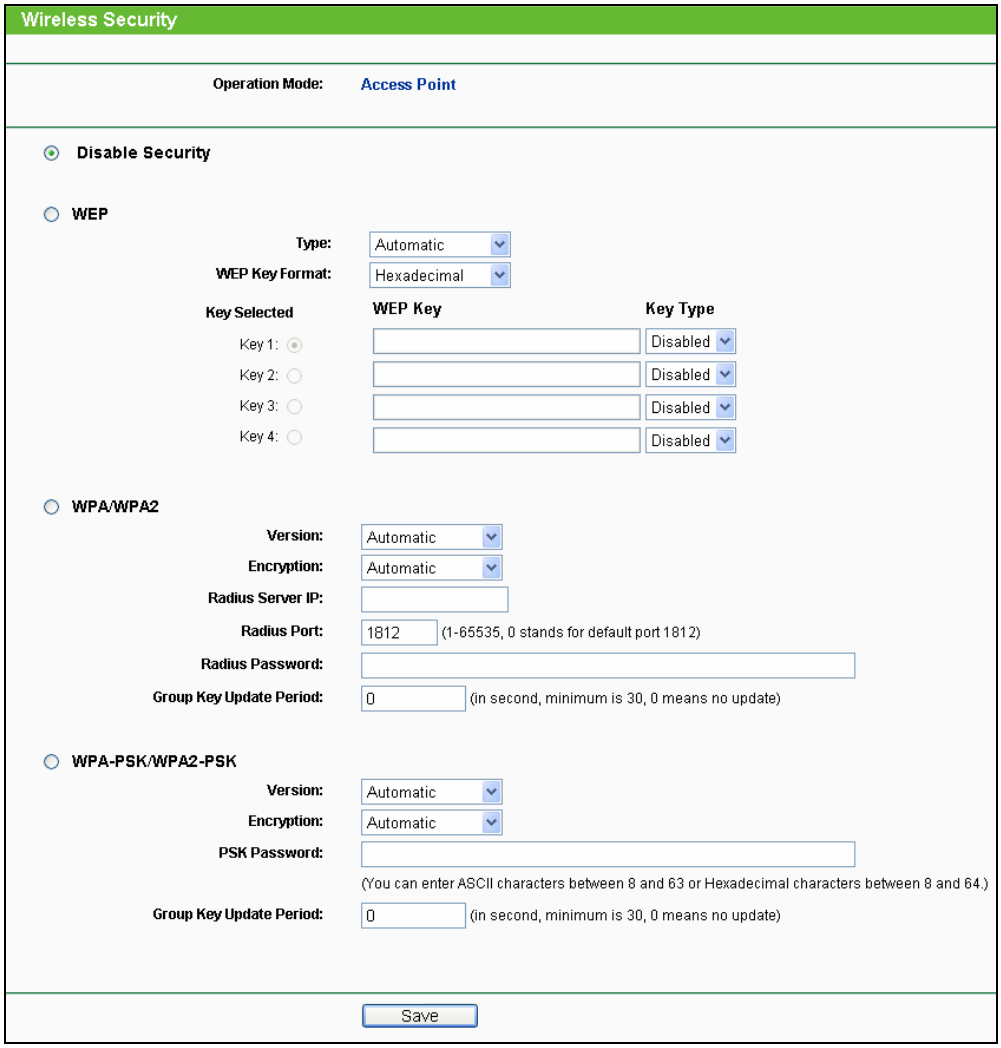


Figure 4-17 Wireless Security - Access Point

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WEP -** Select 802.11 WEP security.
- **WPA-PSK -** Select WPA based on pre-shared passphrase.
- **WPA -** Select WPA based on Radius Server.

Each security option has its own settings as described follows:

- **WEP**

- **Type - You can select one of following types:**

 Automatic - Select Shared Key or Open System authentication type automatically based on the wireless station's capability and request.

Shared Key - Select 802.11 Shared Key authentications.

Open System - Select 802.11 Open System authentication.

- **WEP Key Format -** You can select ASCII or Hexadecimal format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key settings -** Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type -** You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

 For 64-bit encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters.

 For 128-bit encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters.

 For 152-bit encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

☞ **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

➢ **WPA/WPA2**

- **Version -** You can select one of following versions:

 Automatic - Select WPA or WPA2 automatically based on the wireless station's capability and request.

 WPA - Wi-Fi Protected Access.

 WPA2 - WPA version 2.
- **Encryption -** You can select either Automatic, or TKIP or AES.
- **Radius Server IP -** Enter the IP address of the Radius Server.
- **Radius Port -** Enter the port that radius service uses.
- **Radius Password -** Enter the password for the Radius Server.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

➢ **WPA-PSK/WPA2-PSK**

- **Version -** You can select one of following versions:

 Automatic - Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request.

 WPA-PSK - Pre-shared key of WPA.

 WPA2-PSK - Pre-shared key of WPA2.

- **Encryption -** You can select either Automatic, or TKIP or AES.
- **PSK Password -** You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

2) Multi-SSID

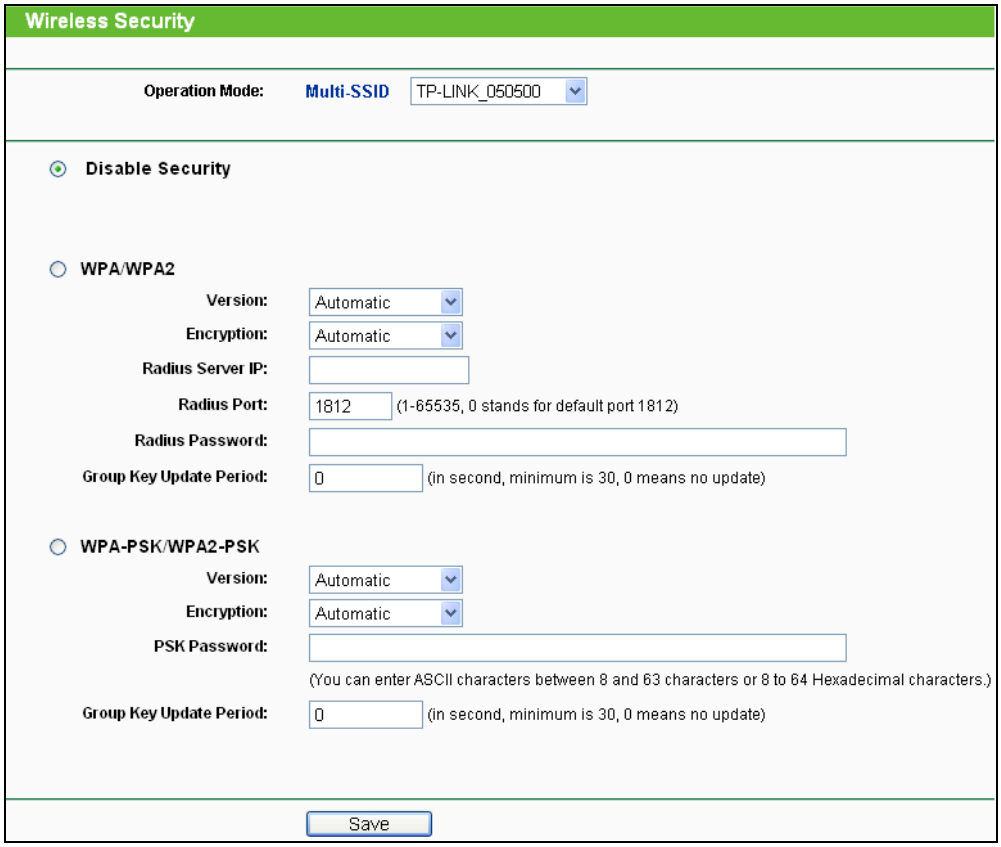


Figure 4-18 Wireless Security – Multi-SSID

➢ **Operation Mode -** Shows the current operation mode. You can choose one of the 4 SSID from the pull-down list.

- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.

- **WPA/WPA2 -** Select WPA/WPA2 based on Radius Server.

- **Version -** You can select one of following versions.

 Automatic - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.

 WPA - Wi-Fi Protected Access.

 WPA2 - WPA version 2.

- **Encryption** - You can select **Automatic**, **TKIP** or **AES**.
- **Radius Server IP** - Enter the IP address of the Radius Server.
- **Radius Port** - Enter the port used by radius service.
- **Radius Password** - Enter the password for the Radius Server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

☞ **Note:**

This security option will become unavailable, if the **Enable VLAN** box in Figure 3-13 is checked.

- **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version** - You can select one of following versions.

 Automatic - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

 WPA-PSK - Pre-shared key of WPA.

 WPA2-PSK - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

☞ **Note:**

You will be reminded to reboot the device after clicking the **Save** button.

3) Client

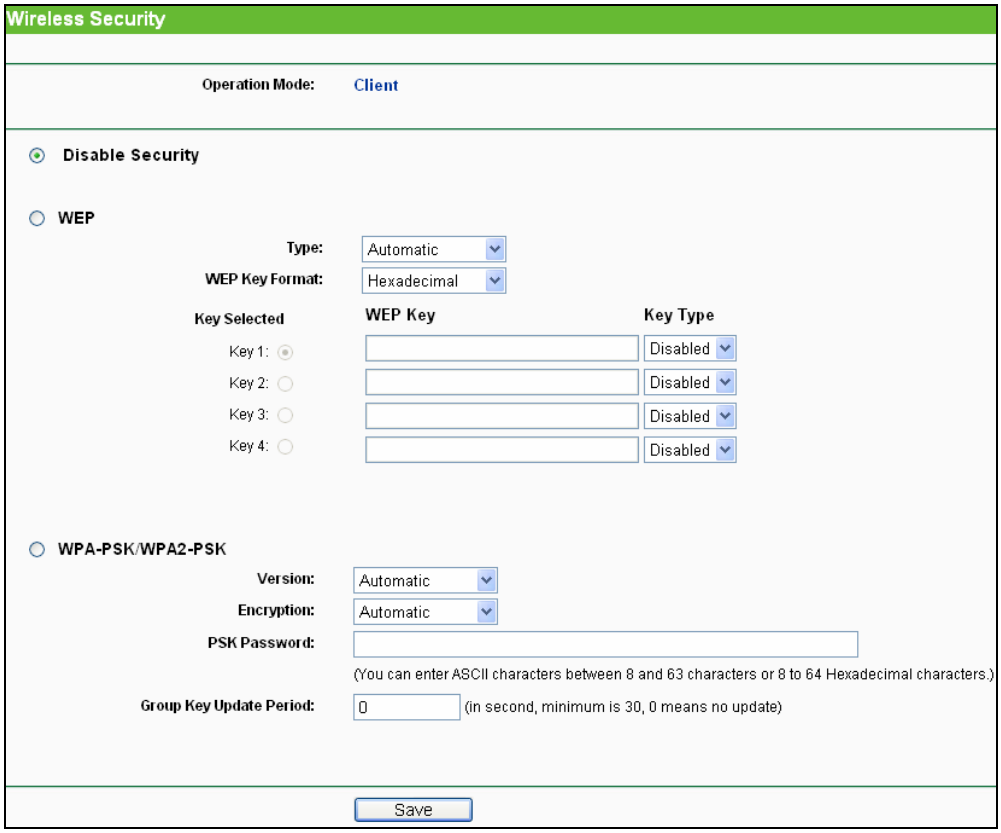


Figure 4-19 Wireless Security – Client

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.
- **Type** - You can select one of following types.

 Automatic - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

 Shared Key - Select 802.11 **Shared Key** authentication type.

 Open System - Select 802.11 **Open System** authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

- **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version** - You can select one of following versions.

 Automatic - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

 WPA-PSK - Pre-shared key of WPA.

 WPA2-PSK - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select **Automatic**, **TKIP** or **AES** as **Encryption**.

- **PSK Passphrase** - Enter a passphrase here.

- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

☞ **Note:**

You will be reminded to reboot the device after clicking the **Save** button.

4) Repeater

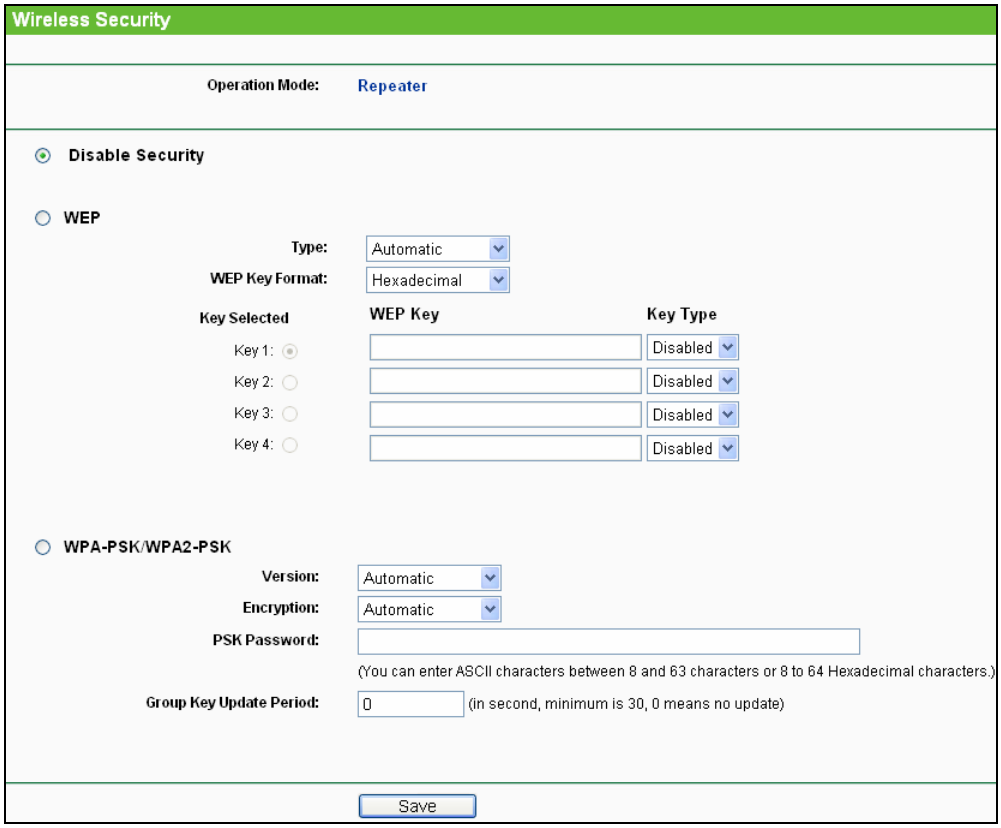


Figure 4-20 Wireless Security – Repeater

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.

- **Type** - You can select one of following types.

 Automatic - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

 Shared Key - Select 802.11 **Shared Key** authentication type.

 Open System - Select 802.11 Open System authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

- **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version** - You can select one of following versions.

 Automatic - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

 WPA-PSK - Pre-shared key of WPA.

 WPA2-PSK - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select **Automatic**, **TKIP** or **AES** as **Encryption**.

- **PSK Passphrase** - Enter a passphrase here.

- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

☞ **Note:**

You will be reminded to reboot the device after clicking the **Save** button.

5) Universal Repeater

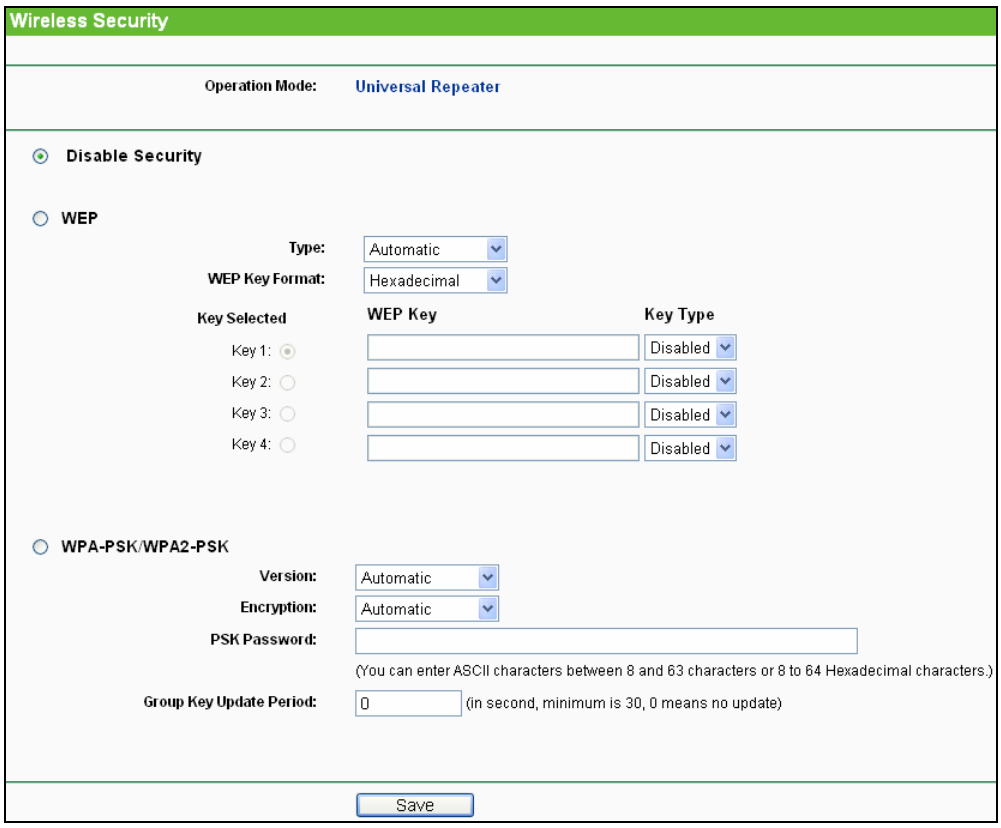


Figure 4-21 Wireless Security – Universal Repeater

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.
- **Type** - You can select one of following types.

 Automatic - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

 Shared Key - Select 802.11 **Shared Key** authentication type.

 Open System - Select 802.11 Open System authentication.
- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.

- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

 For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

 For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

 For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

➢ **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared key.

- **Version** - You can select one of following versions.

 Automatic - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

 WPA-PSK - Pre-shared key of WPA.

 WPA2-PSK - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type**, you can select **Automatic**, **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - Enter a passphrase here.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

☞ **Note:**

You will be reminded to reboot the device after clicking the **Save** button.



Figure 4-22 Wireless Security – Bridge with AP

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.

- **Type** - You can select one of following types.

 Automatic - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

 Shared Key - Select 802.11 **Shared Key** authentication type.

 Open System - Select 802.11 Open System authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.

For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.

For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

1. If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.
2. You will be reminded to reboot the device after clicking the **Save** button.

4.7.3 Wireless MAC Filtering

Selecting **Wireless > Wireless MAC Filtering** will allow you to set up some filtering rules to control wireless stations accessing the device, which depend on the station's MAC address on the following screen as shown in Figure 4-23. As the configuration is the same in each operation mode, here we just take the Access Point for example.

☞ **Note:**

This function is not available when the operation is set to Client.

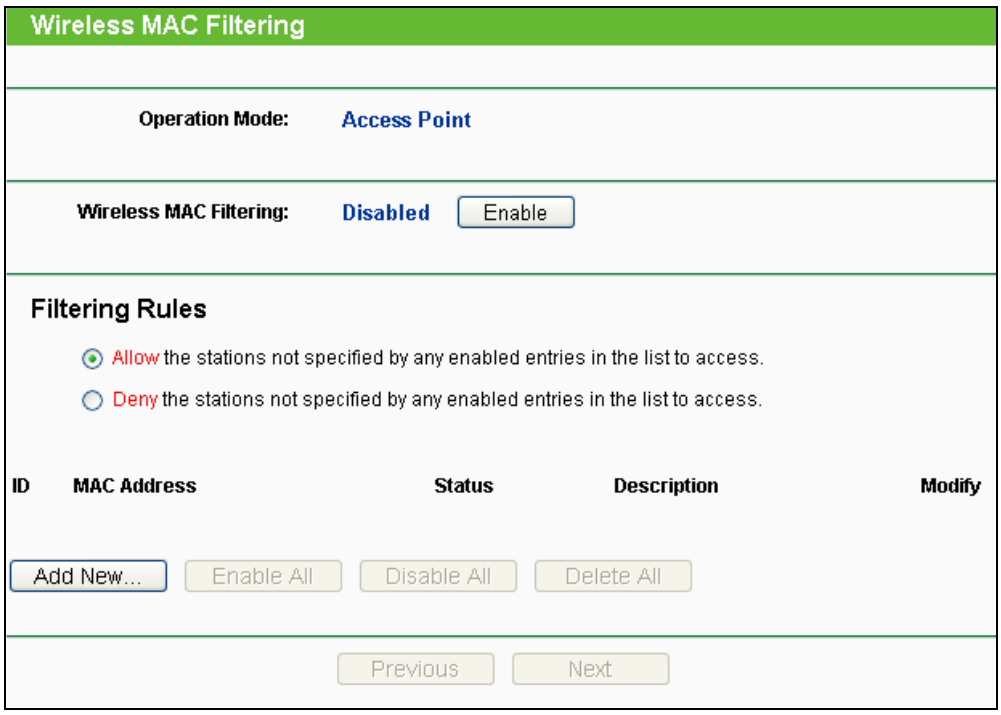


Figure 4-23 Wireless MAC address Filtering

➢ **Operation Mode -** Shows the current operation mode.

- **Wireless MAC Filtering -** Click the **Enable** button to enable the Wireless MAC Address Filtering. The default setting is disabled.

- To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-24.

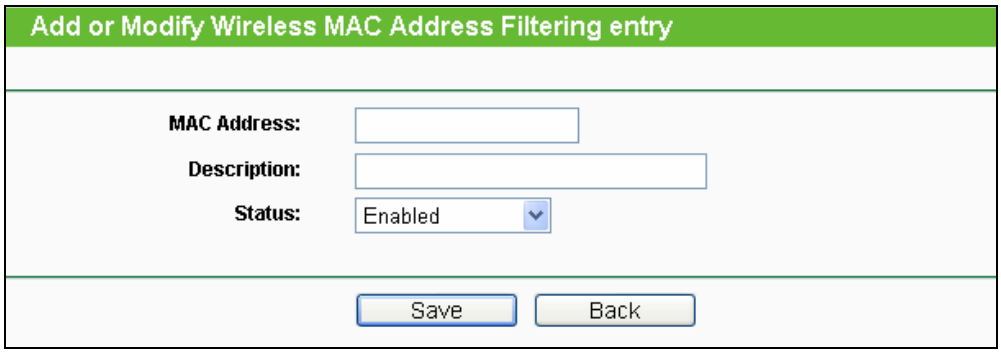


Figure 4-24 Add or Modify Wireless MAC Address Filtering entry

- **MAC Address -** Enter the wireless station's MAC address that you want to control.

- **Description -** Give a simple description of the wireless station.

- **Status -** Select a status for this entry, either **Enabled** or **Disabled**.

- To set up an entry, click **Enable**, and follow these instructions:

1. First, you must decide whether the unspecified wireless stations can or cannot access the AP;
2. If you desire that the unspecified wireless stations can access the AP, please select the radio button **Allow the stations not specified by any enabled entries in the list to access**;
3. Otherwise, select the radio button **Deny the stations not specified by any enabled entries in the list to access**.

- To Add a Wireless MAC Address filtering entry, clicking the **Add New...** button, and following these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example, 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example, Wireless station A.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

- To add another entries, repeat steps 1~4.

➢ To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all the Entries enabled.

Click the **Disable All** button to make all the Entries disabled.

Click the **Delete All** button to delete all the entries.

Click the **Next** button to go to the next page.

Click the **Previous** button to return to the previous page.

☞ **Note:**

1. If you enable the function and select the **Deny the stations not specified by any enabled entries in the list to access** for Filtering Rules, there will be not any enable entries in the list; thus, no wireless stations can access the AP.
2. Only in Standard AP mode, the current operation mode is shown at the top. Besides, if Multi-SSID, a sub mode of Standard AP, is selected, you can choose one of the 4 SSIDs from the pull-down list.

4.7.4 Wireless Advanced

Selecting **Wireless > Wireless Advanced** will allow you to do some advanced settings for the device in the following screen as shown in Figure 4-25. As the configuration for each operation mode is almost the same, we take Access Point mode for example here.

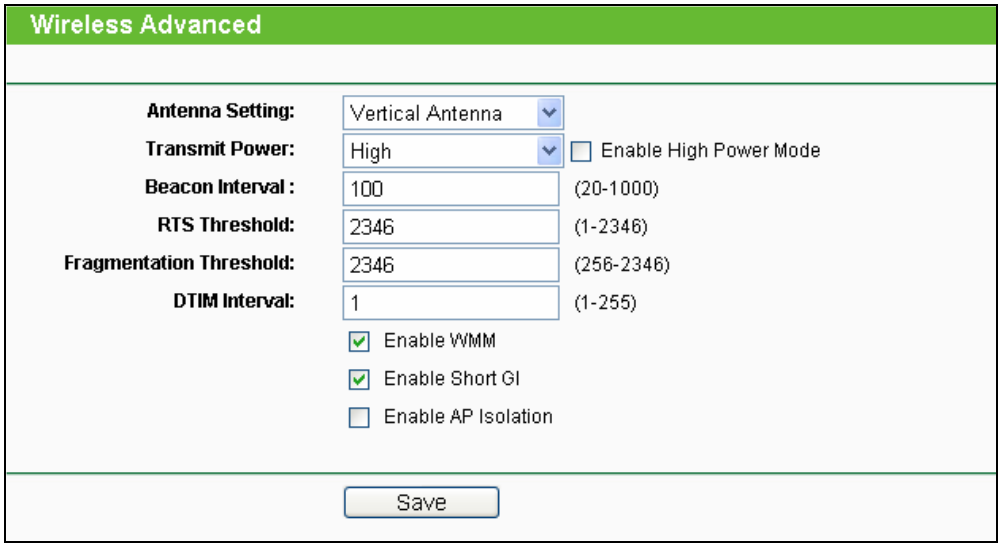


Figure 4-25 Wireless Advanced

- **Antenna Settings -** The polarization of an antenna. You can select Vertical Antenna, Horizontal Antenna or External Antenna.
- **Transmit Power -** Here you can specify the transmit power of the Device. You can select High, Middle or Low whichever you would like. High is the default setting and is recommended.
- **Beacon Interval -** The beacons are the packets sent by the Device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 20-1000 milliseconds. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM -** WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI -** This function is recommended, for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation -** Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

Note:

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

4.7.5 Antenna Alignment

Selecting **Wireless > Antenna Alignment** will shows how remote AP's signal strength changes while changing the antenna's direction.

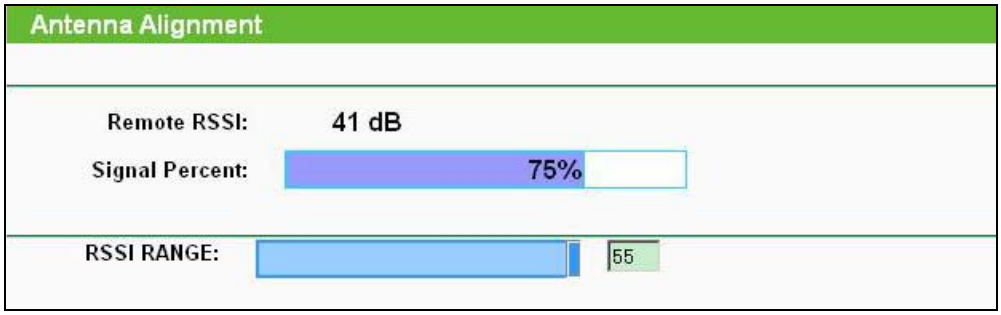


Figure 4-26 Antenna Alignment

- **Remote AP RSSI**- Remote AP's signal strength value.
- **Signal percent**- The ratio of RSSI to RSSI RANGE in percentage.
- **RSSI RANGE**- You can drag the Slider to set or input the RSSI RANGE value.

Note:

It only works after you have established connection to remote AP in client mode.

4.7.6 Distance Settings

Selecting **Wireless > Distance Settings** will adjust the wireless range in outdoor conditions. This is a critical feature required for stabilizing outdoor links.

Enter the distance of your wireless link and the software will optimize the frame ACK timeout value automatically.

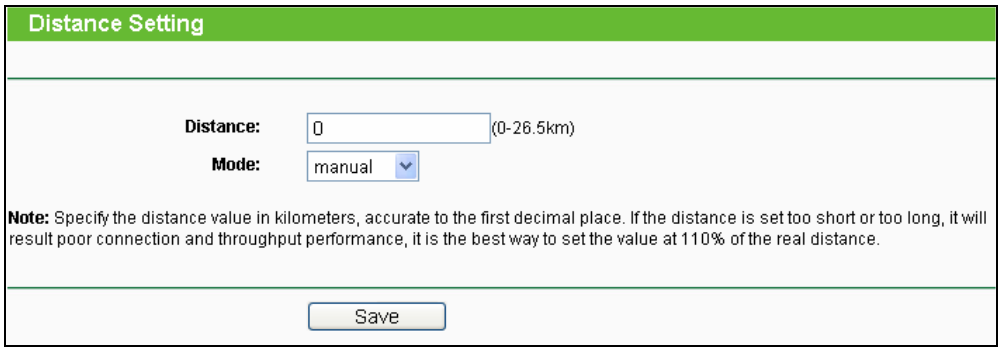


Figure 4-27 Distance Setting

Note:

One hundred-meter is the smallest unit of this setting.

4.7.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in Figure 4-28.

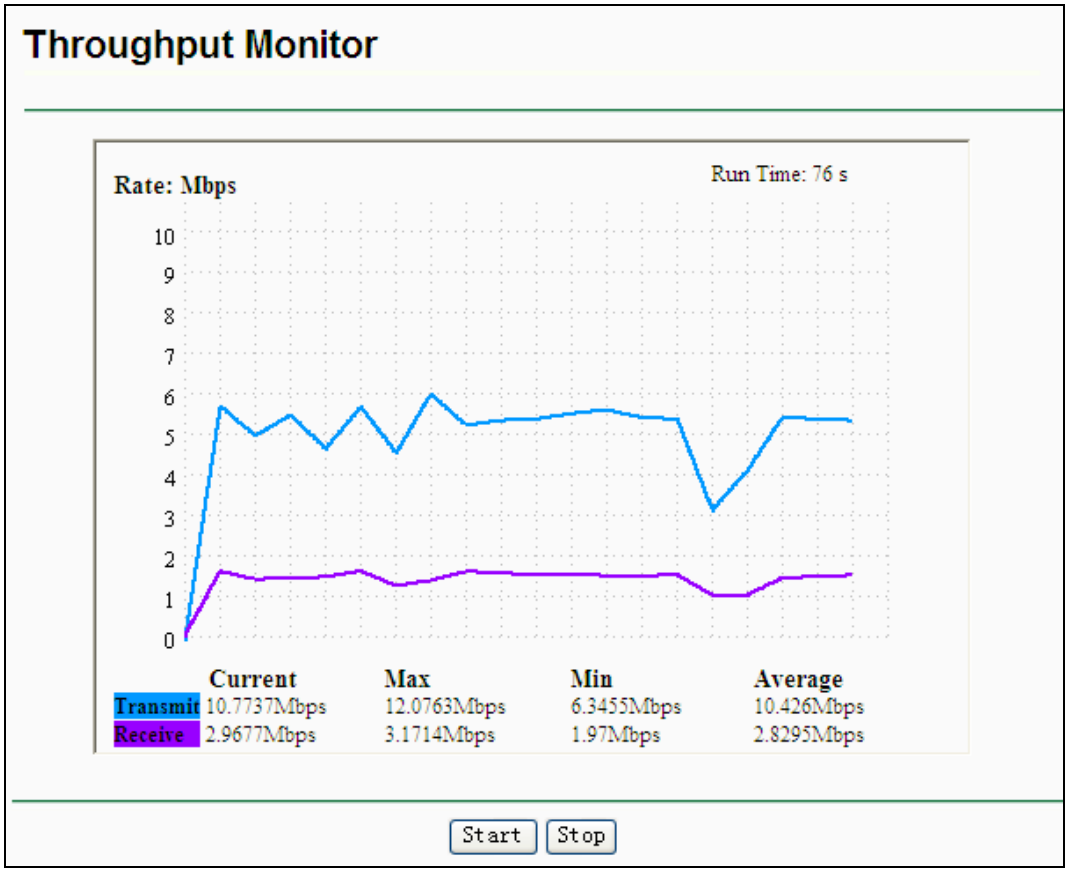


Figure 4-28 Throughput Monitor

- **Rate -** The Throughput unit.
- **Run Time -** How long this function is running.
- **Transmit -** Wireless transmit rate information.
- **Receive -** Wireless receive rate information.

Click the **Start** button to start wireless throughput monitor.

Click the **Stop** button to stop wireless throughput monitor.

4.7.8 Wireless Statistics

Selecting **Wireless > Wireless Statistics** will allow you to see the the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station as shown in Figure 4-29.

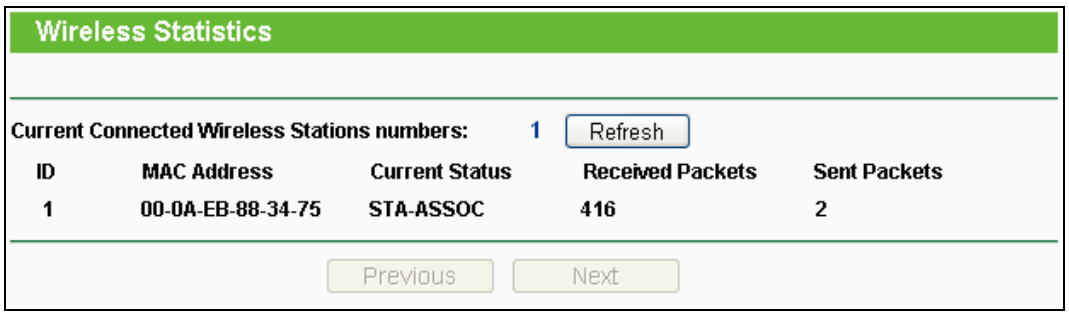


Figure 4-29 Wireless Statistics

- **MAC Address -** the connected wireless station's MAC address.
- **Current Status -** the connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected.
- **Received Packets -** packets received by the station.
- **Sent Packets -** packets sent by the station.
- **Belong To -** the SSID that station belong to.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

Note:

This page will be refreshed automatically every 5 seconds.

4.8 DHCP

The DHCP (Dynamic Host Configuration Protocol) Server will automatically assign dynamic IP addresses to the computers on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

There are three submenus under the DHCP menu (shown as Figure 4-30): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.

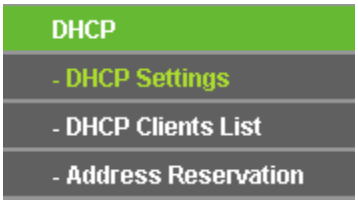


Figure 4-30 The DHCP menu

4.8.1 DHCP Settings

Selecting **DHCP > DHCP Settings** will enable you to set up the AP as a DHCP server, which provides the TCP/IP configuration for all the PCs that are connected to the system on the LAN. The DHCP Server is Disable by default, and can be configured on the page (shown as Figure 4-31):

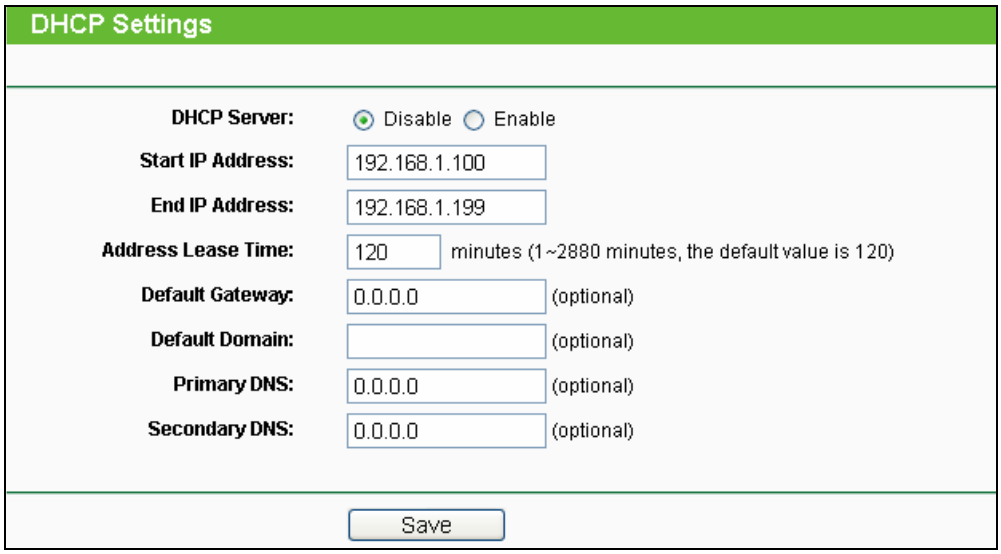


Figure 4-31 DHCP Settings

- **DHCP Server - Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the IP address of the computer manually.
- **Start IP Address -**This field specifies the first address in the IP Address pool. 192.168.1.100 is the default start IP address.
- **End IP Address -** This field specifies the last address in the IP Address pool. 192.168.1.199 is the default end IP address.
- **Address Lease Time –** It is the length of time a network user will be allowed to keep connecting to the device with the current DHCP Address. Enter the amount of time (in minutes), and then the DHCP address will be "leased". The time range is 1~2880 minutes. The default value is 120 minutes.
- **Default Gateway -** (Optional) Input the IP Address of the gateway.
- **Default Domain -** (Optional) Input the domain name of your network.
- **Primary DNS -** (Optional) Input the DNS IP address provided by your ISP or consult your ISP.

- **Secondary DNS -** (Optional) You can input the IP Address of another DNS server if your ISP provides two DNS servers.

Note:

1. When the device is working on Dynamic IP mode, the DHCP Server function will be disabled.
2. To use the DHCP server function of the device, you should configure all computers in the LAN as "**Obtain an IP Address automatically**" mode. This function will take effect until the device reboots.

Click **Save** to save the changes.

4.8.2 DHCP Clients List

Selecting **DHCP > DHCP Clients List** will enable you to view the Client Name, MAC Address, Assigned IP and Lease Time of each DHCP Client connected to the device (Figure 4-32).

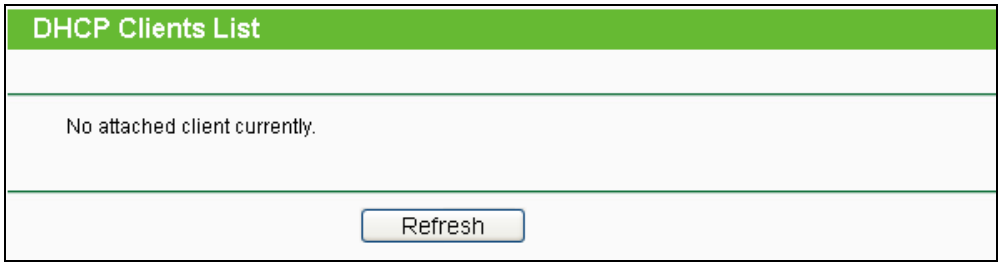


Figure 4-32 DHCP Clients List

- **Client Name -** The name of the DHCP client.
- **MAC Address -** The MAC address of the DHCP client.
- **Assigned IP -** The IP address that the device has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased.

You cannot change any of the values on this page.

To update this page and to show the current connected devices, click on the **Refresh** button.

4.8.3 Address Reservation

Selecting **DHCP > Address Reservation** will enable you to specify a reserved IP address for a PC on the LAN, so the PC will always obtain the same IP address each time when it accesses the AP. Reserved IP addresses should be assigned to servers that require permanent IP settings. The screen below is used for address reservation (shown in Figure 4-33).

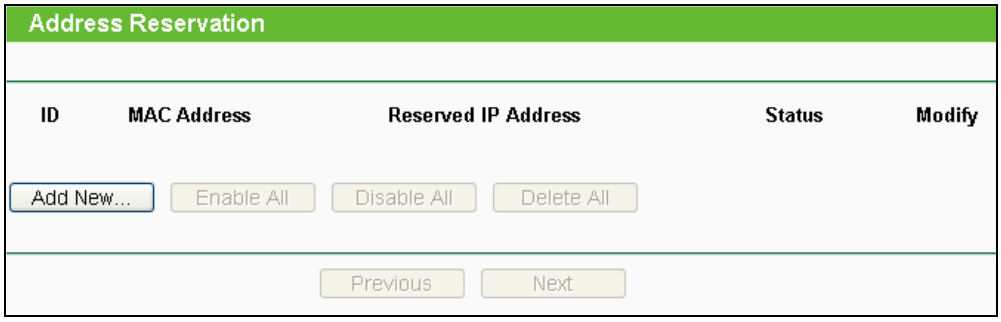


Figure 4-33 Address Reservation

- **MAC Address -** The MAC Address of the PC that you want to reserve an IP address for.
- **Reserved IP Address -** The IP address that the device reserved.
- **Status -** It shows whether the entry is enabled or not.
- **Modify -** To modify or delete an existing entry.

- To Reserve IP Addresses, you can follow these steps:

1. Click the **Add New...** button to add a new Address Reservation entry.
2. Enter the MAC Address (the format for the MAC Address is XX-XX-XX-XX-XX-XX.) and the IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button.

- To modify a Reserved IP Address, you can follow these steps:

1. Select the reserved address entry as you desired, **modify** it. If you wish to delete the entry, click the **Delete** link of the entry.
2. Click the **Save** button.

Click the **Add New...** button to add a new Address Reservation entry.

Click the **Enable All** button to enable all the entries in the table.

Click the **Disable All** button to disable all the entries in the table.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Note:

The changes will not take effect until the device reboots.

4.9 System Tools

The **System Tools** option helps you to optimize the configuration of your device.

There are ten submenus under the **System Tools** menu (shown as Figure 4-34): **SNMP**, **Diagnostic**, **Ping Watch Dog**, **Speed Test**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, and **System Log**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 4-34 The System Tools menu

4.9.1 SNMP

Selecting **System Tools > SNMP** will allow you to configure some parameters (as shown in Figure 4-35), so that you can use this SNMP (Simple Network Management Protocol) function allowing the network management station to retrieve statistics and status from the SNMP agent in this device.

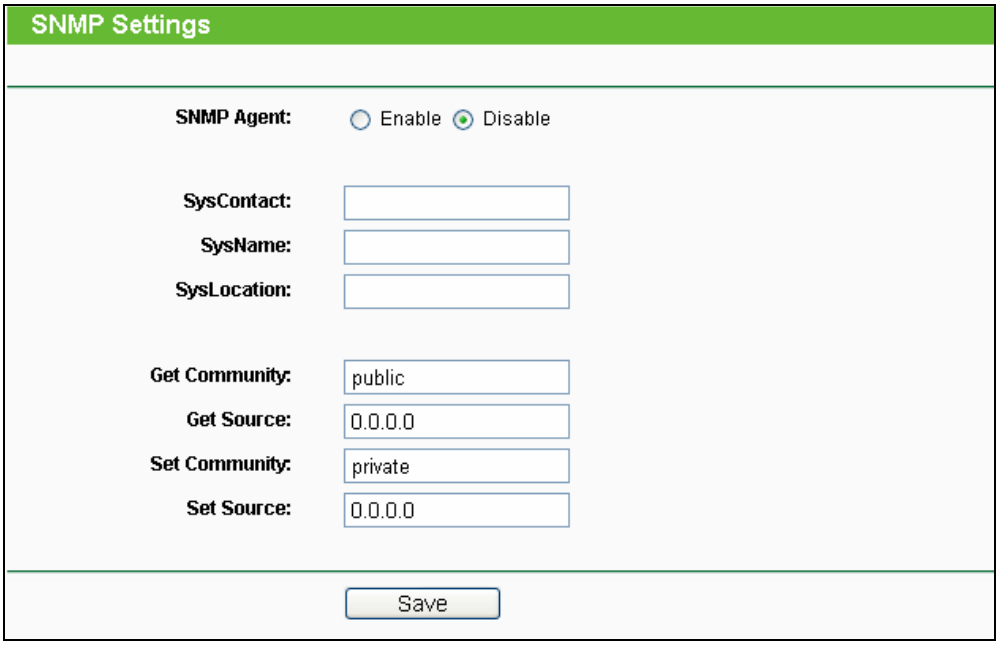


Figure 4-35 SNMP Settings

- **SNMP Agent -** Choose **Enable** to open this function if you want to have remote control through SNMPv1/v2 agent with MIB-II. Choose **Disable** to close this function.
- **SysContact -** The textual identification of the contact person for this managed node.
- **SysName -** An administratively-assigned name for this managed node.
- **SysLocation -** The physical location of this node.

Note:

Specifying one of these values via the Device's Web-Based Utility makes the corresponding object read-only. If there isn't such a config setting, then the write request will succeed (assuming suitable access control settings), but the new value would be forgotten the next time the agent was restarted.

- **Get Community -** Enter the community name that allows Read-Only access to the Device's SNMP information. The community name can be considered a group password. The default setting is **public**.
- **Get Source -** Defines the IP address or subnet for management systems that can read information from this 'get' community device.
- **Set Community -** Enter the community name that allows Read/Write access to the Device's SNMP information. The community name can be considered a group password. The default setting is **private**.
- **Set Source -** Defines the IP address or subnet for management systems that can control this 'set' community device.

Note:

A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If an IP Address of 0.0.0.0 is specified, the agent will accept all requests under the corresponding community name.

Click the **Save** button to save your settings.

4.9.2 Diagnostic

Selecting **System Tools > Diagnostic** allows you to check the connections of your network components on the screen shown in Figure 4-36.

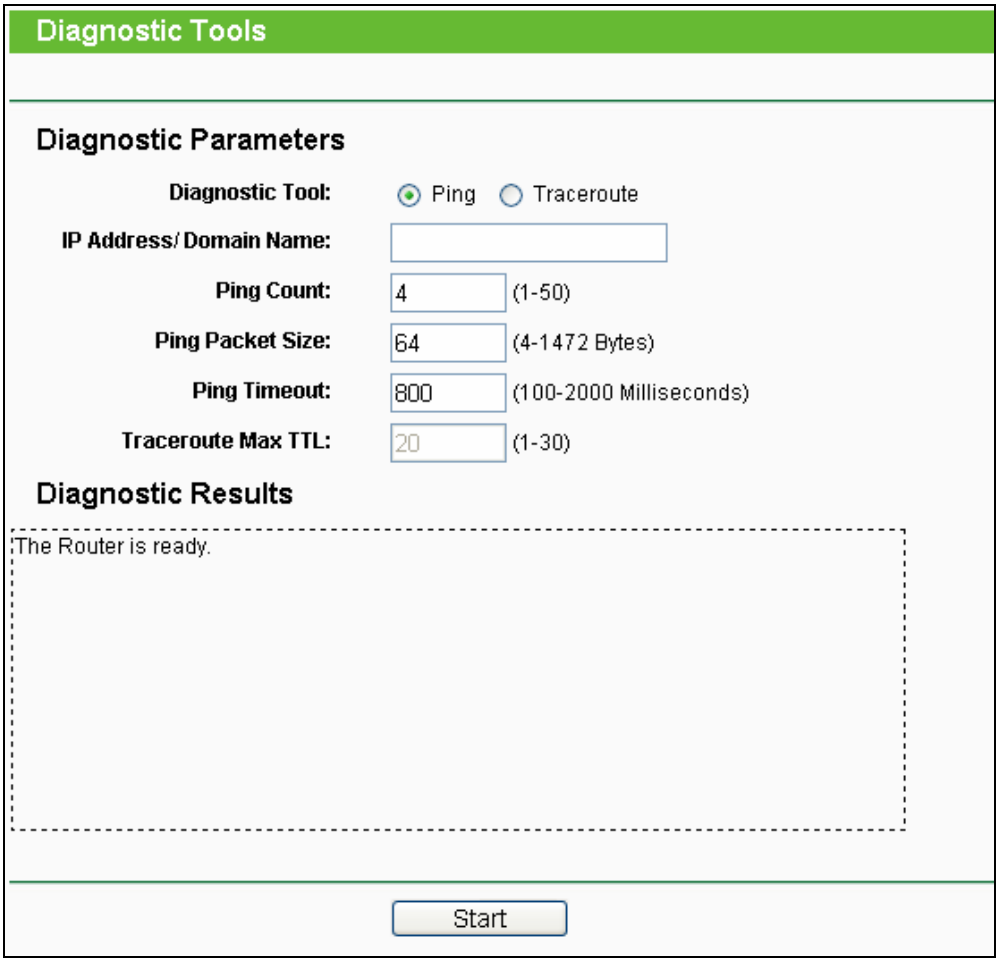


Figure 4-36 Diagnostic Tool

- **Diagnostic Tool -** Click the radio button to select one diagnostic tool:

- **Ping -** This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.

- **Traceroute -** This diagnostic tool tests the performance of a connection.

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/ Domain Name** - Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
- **Ping Count** - Specifies the number of Echo Request messages sent. The default is 4.
- **Ping Packet Size** - Specifies the number of data bytes to be sent. The default is 64.
- **Ping Timeout** - Time to wait for a response, in milliseconds. The default is 800.
- **Traceroute Max TTL** - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click the **Start** button to start the diagnostic procedure.

The **Diagnostic Results** page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

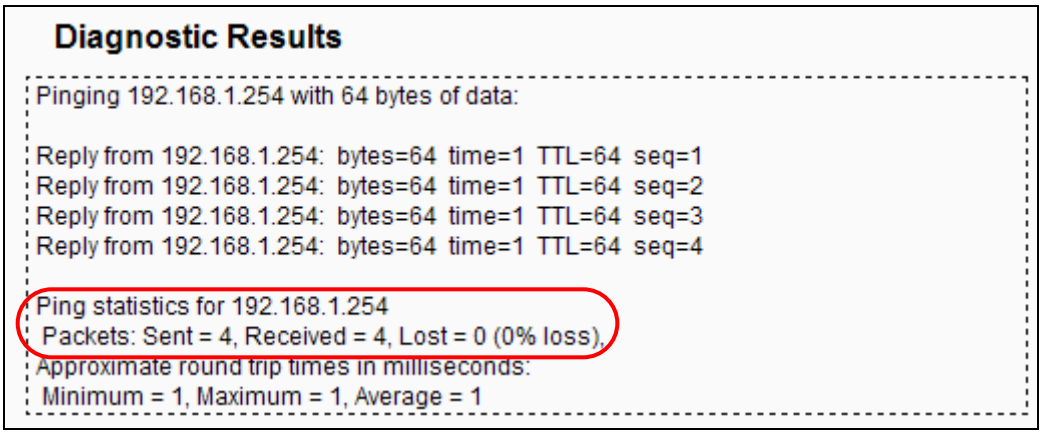


Figure 4-37 Diagnostic Results

Note:

1. Only one user can use the diagnostic tools at one time.
2. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters, and "Traceroute Max TTL" is Traceroute Parameter.

4.9.3 Ping Watch Dog

Selecting **System Tools > Ping Watch Dog** allows you to continuously monitor the particular connection between the device and a remote host. It makes this device continuously ping a user defined IP address (it can be the Internet gateway for example.). If it is unable to ping under the user defined constraints, this device will automatically reboot.

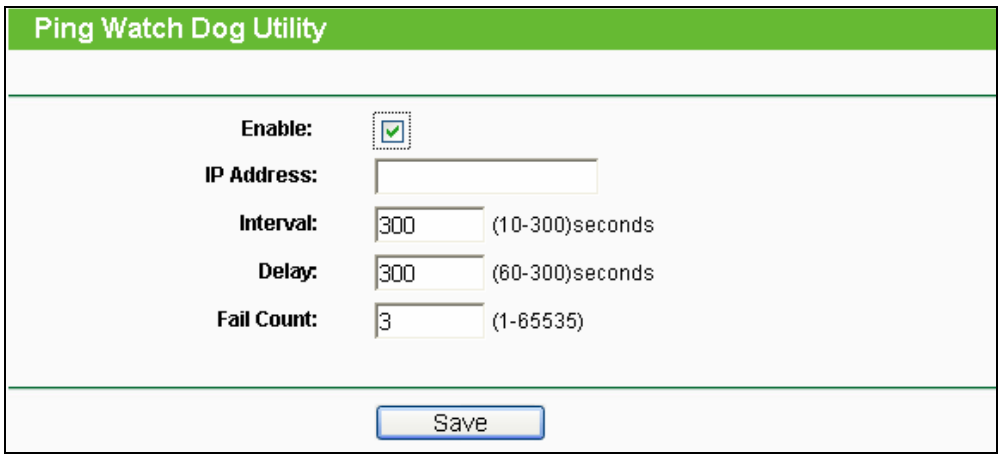


Figure 4-38 Ping Watch Dog Utility

- **Enable -** Turn on/off Ping Watch Dog.
- **IP Address -** The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval -** Time internal between two ping packets which are sent out continuously.
- **Delay -** Time delay before first ping packet is sent out when the device is restarted.
- **Fail Count –** It is the upper limit of the ping packet the device can drop continuously. If this value is overrun, the device will restart automatically.

Be sure to click the **Save** button to make your settings in operation.

4.9.4 Speed Test

Selecting **System Tools > Speed Test** helps to test the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other.

It should be used for the preliminary throughput estimation between two network devices.

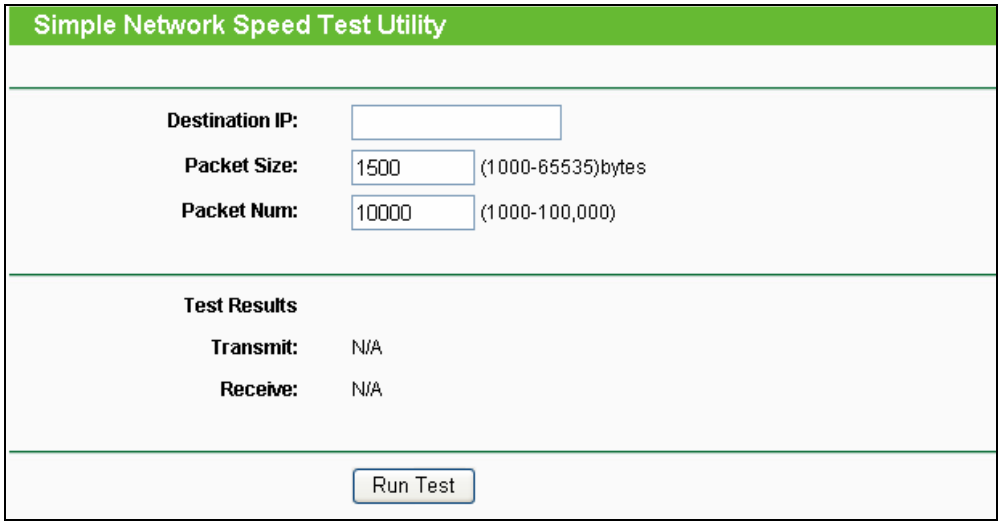


Figure 4-39 Speed Test Utility

- **Destination IP-**The Remote device's IP address
- **Transmit -** Estimate the outgoing throughput (Tx).
- **Receive -** Estimate the ingoing throughput (Rx).

Be sure to click the **Run Test** button to start a new test after you fill enough information. You can also stop a running test by click **Stop Test** button at any time.

4.9.5 Firmware Upgrade

Selecting **System Tools > Firmware Upgrade** allows you to upgrade the latest version of firmware for the device on the screen shown in Figure 4-40.

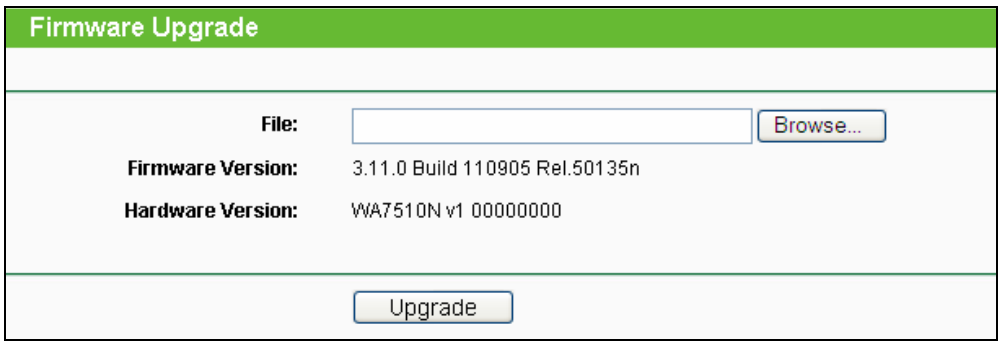


Figure 4-40 Firmware Upgrade

- **Firmware Version -** Displays the current firmware version.
- **Hardware Version** - It displays the current hardware version.
- To upgrade the Device's firmware, follow these instructions:

1. Download a most recent firmware upgrade file from our website (www.tp-link.com).

2. Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
3. Click the **Upgrade** button.
4. The Device will reboot while the upgrading has been finished.

☞ **Note:**

1. The firmware version must correspond to the hardware.
2. The upgrade process takes a few moments and the Device restarts automatically when the upgrade is complete.
3. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the Device.

4.9.6 Factory Defaults

Selecting **System Tools > Factory Default** allows you to restore the factory default settings for the device on the screen shown in Figure 4-41.



Figure 4-41 Restore Factory Defaults

Click the **Restore** button to reset all configuration settings to their default values.

- Default User Name **- admin**.
- Default Password **- admin**.
- Default IP Address **- 192.168.1.254**.
- Default Subnet Mask **- 255.255.255.0**.

☞ **Note:**

All changed settings will be lost when defaults are restored.

4.9.7 Backup & Restore

Selecting **System Tools > Backup & Restore** allows you to save all configuration settings to your local computer as a file or restore the device's configuration on the screen shown in Figure 4-42.



Figure 4-42 Save or Restore the Configuration

Click **Backup** to save all configuration settings to your local computer as a file.

➢ To restore the device's configuration, follow these instructions:

1. Click **Browse…** to find the configuration file which you want to restore.
2. Click **Restore** to update the configuration with the file whose path is the one you have input or selected in the blank.

Note:

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged.

The restoring process lasts for 20 seconds and the AP will restart automatically then.

Keep the power of the AP on during the process, in case of any damage.

4.9.8 Reboot

Selecting **System Tools > Reboot** allows you to reboot the device on the screen as shown in Figure 4-43.



Figure 4-43 Reboot the device

Click the **Reboot** button to reboot the Device.

➢ Some settings of the Device will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically.).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Device (system will reboot automatically.).
- Restore the Device's settings to the factory defaults (system will reboot automatically.).
- Update the configuration with the file (system will reboot automatically.).

4.9.9 Password

Selecting **System Tools > Password** allows you to change the factory default user name and password of the device on the screen shown in Figure 4-44.

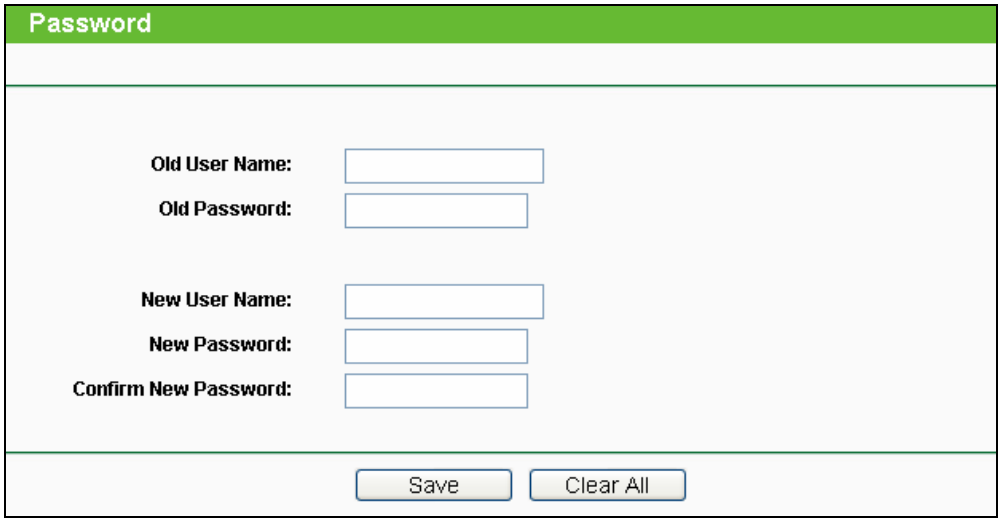


Figure 4-44 Password

It is strongly recommended that you change the factory default user name and password of the AP. All users who try to access the AP's web-based utility will be prompted for the AP's user name and password.

☞ **Note:**

The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

4.9.10 System Log

Selecting **System Tools > System Log** allows you to query the Logs of the device on the screen shown in Figure 4-45.

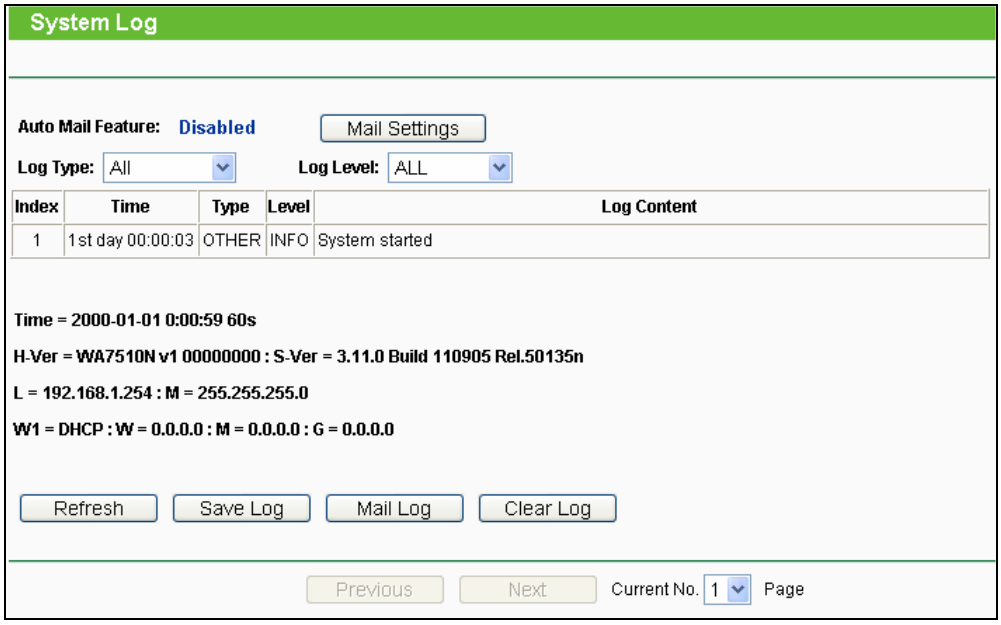


Figure 4-45 System Log

- **Auto Mail Feature -** Indicates whether auto mail feature is enabled or not.
- **Mail Settings -** Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.
- **Log Type -** By selecting the log type, only logs of this type will be shown.
- **Log Level -** By selecting the log level, only logs of this level will be shown.
- **Refresh -** Refresh the page to show the latest log list.
- **Save Log -** Click to save all the logs in a txt file.
- **Mail Log -** Click to send an email of current logs manually according to the address and validation information set in Mail Settings. The result will be shown in the later log soon.
- **Clear Log -** All the logs will be deleted from the Device permanently, not just from the page.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Chapter 5 Configuring AP Router & AP Client Router Mode

This chapter will show each Web page's key functions and the configuration way in AP Router mode as well as AP Client Router mode.

Note:

The setting Web pages of these two modes are mostly the same, with only three differences:

1. In AP Router Mode, there is one more WAN connection type, **Big Pond Cable**, than that in AP Client Router Mode.（See Section 5.6.2）
2. In AP Client Router Mode, there is one more submenu under Wireless main menu, **Antenna Alignment**, than that in AP Router Mode, as shown in Figure 5-24 & Figure 5-25. (See Section 5.7)
3. The **Wireless Settings** page in AP Router mode and that in AP Client Router mode are something different, as shown in Figure 5-26 & Figure 5-27. (See Section 5.7.1)

5.1 Login

Open your web browser. Type in the default address http://192.168.1.254 in the address field of web browser and then press **Enter**.



Figure 5-1 Login to the Device

Enter **admin** for the User Name and Password (both in lower case letters) in Figure 5-2 below. Then click **OK** or press Enter.

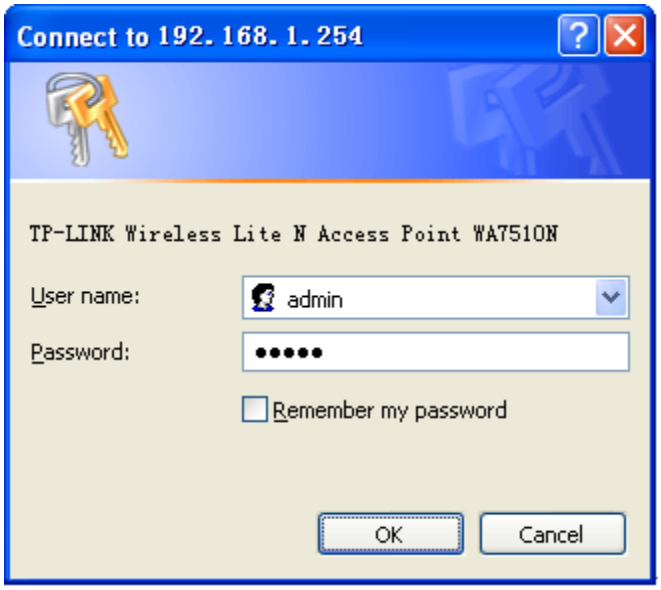


Figure 5-2 Login Windows

Note:

If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings**, in the screen that appears, cancel the **Using Proxy** checkbox, and click **OK** to finish it.

After a successful login, you can configure and manage the device. There are sixteen main menus on the leftmost column of the web-based management page as in Figure 5-3: **Status**, **Quick Setup**, **QSS**, **Operation Mode**, **Network**, **Wireless**, **DHCP, Forwarding, Security, Parental Control, Access Control, Static Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS** and **System Tools**. Submenus will be available after clicking one of the main menus. On the right of the web-based management page lays the detailed explanations and instructions for the corresponding page.

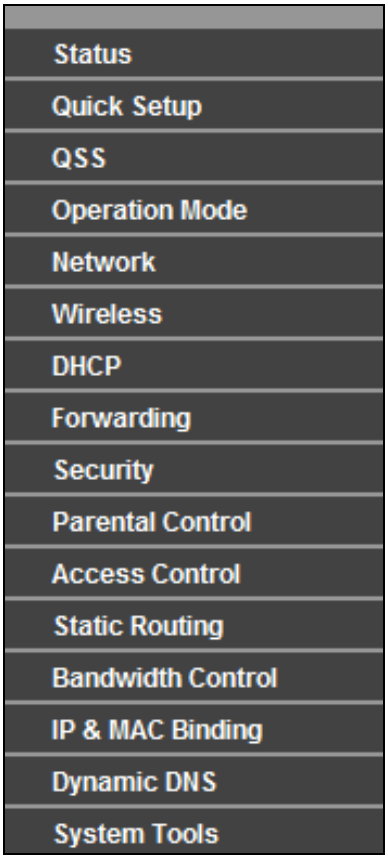


Figure 5-3 the Main Menu

5.2 Status

The **Status** page displays the Device's current status and configuration, all information which is read-only.

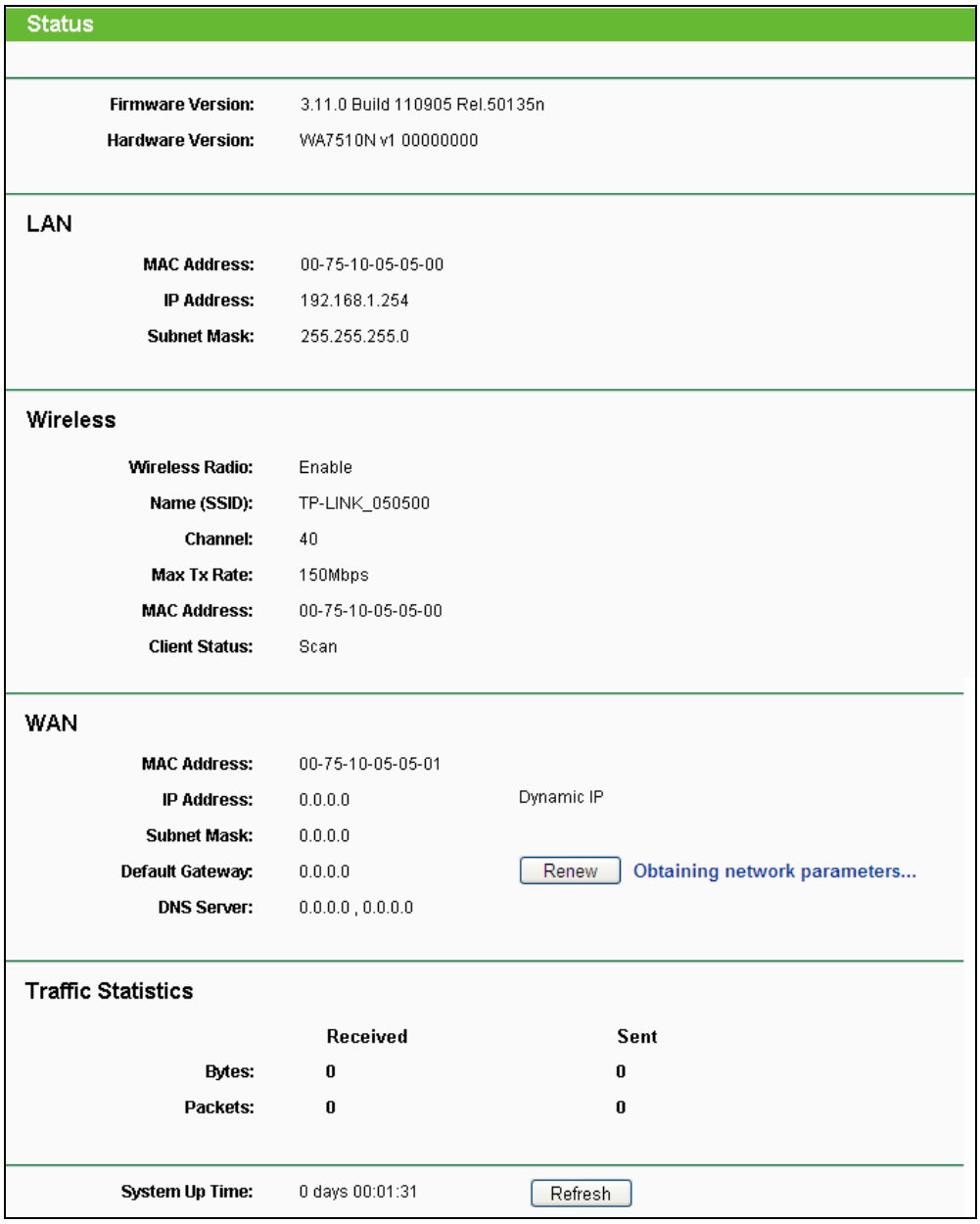


Figure 5-4 Status

- **LAN** - The following parameters apply to the LAN port of the Device. You can configure them in the **Network -> LAN** page.
 - **MAC Address**- The physical address of the Device, as seen from the LAN.
 - **IP Address**- The LAN IP address of the Device.
 - **Subnet Mask** - The subnet mask associated with LAN IP address.
- **Wireless** - These are the current settings or information for Wireless. You can configure them in the **Wireless -> Wireless Settings** page.
 - **Wireless Radio**- Indicates whether the wireless radio feature of the Device is enabled or disabled.
 - **Name (SSID)** - The SSID of the Device.

- **Channel** - The current wireless channel in use.
- **Mode** - The current wireless mode which the Device works on.
- **Max Tx Rate** - The maximum tx rate.
- **MAC Address** - The physical address of the Device, as seen from the WLAN.
- **Client Status** - The status of client.

 Init: Connection is down; Scan: Try to find the AP; Auth: Try to authenticate; ASSOC: Try to associate; Run: Associated successfully.

➢ **WAN** - The following parameters apply to the WAN ports of the Device. You can configure them in the **Network -> WAN** page.

- **MAC Address**- The physical address of the WAN port, as seen from the Internet.
- **IP Address** - The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to Internet.
- **Subnet Mask** - The subnet mask associated with the WAN IP Address.
- **Default Gateway** - The Gateway currently used by the Device is shown here. When you use **Dynamic IP** as the connection Internet type, the **Renew** button will be displayed here. Click the **Renew** button to obtain new IP parameters dynamically from the ISP. And if you have got an IP address, **Release** button will be displayed here. Click the **Release** button to release the IP address the Device has obtained from the ISP.
- **DNS Server** - The DNS (Domain Name System) Server IP addresses currently used by the Device. Multiple DNS IP settings are common. Usually, the first available DNS Server is used.
- **Online Time** - The time that you are online. When you use **PPPoE** as WAN connection type, the online time is displayed here. Click the **Connect** or **Disconnect** button to connect to or disconnect from Internet.

➢ **Secondary Connection** - Besides PPPoE, if you use an extra connection type to connect to a local area network provided by ISP, then parameters of this secondary connection will be shown in this area.

➢ **Traffic Statistics** - The Device's traffic statistics.

- **Sent (Bytes)** - Traffic that counted in bytes has been sent out from the WAN port.
- **Sent (Packets)** - Traffic that counted in packets has been sent out from WAN port.
- **Received (Bytes)** - Traffic that counted in bytes has been received from the WAN port.
- **Received (Packets)** - Traffic that counted in packets has been received from the WAN port.

➢ **System Up Time** - The length of the time since the Device was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Device.

5.3 Quick Setup

Please refer to Section 3.2 Quick Setup – 3.2.2 AP Router Mode or Section 3.2 Quick Setup – 3.2.3 AP Client Router Mode for more details.

5.4 QSS

This section will guide you to add a new wireless device to an existing network quickly by **QSS (Quick Secure Setup)** function.

Select menu **QSS,** then you will see the next screen (shown in Figure 5-5).

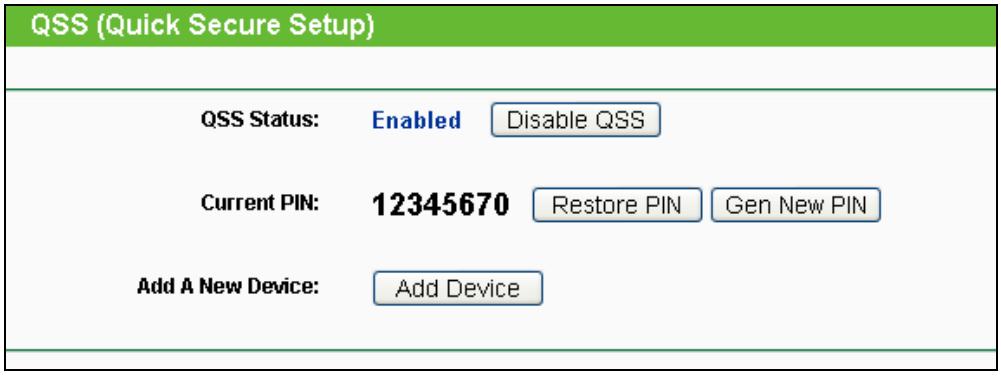


Figure 5-5 QSS

- **QSS Status** - Enable or disable the QSS function here.
- **Current PIN** - The current value of the Device's PIN displayed here. The default PIN of the Device can be found in the label or User Guide.
- **Restore PIN** - Restore the PIN of the Device to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the Device's PIN. You can ensure the network security by generating a new PIN.
- **Add A New Device** - You can add the new device to the existing network manually by clicking **Add Device** button.

Note:

The **QSS** function cannot be configured if the Wireless Function of the Device is disabled. Please make sure the Wireless Function is enabled before configuring the **QSS**.

- **To add a new device:**

1. If the new device supports Wi-Fi Protected Setup and is equipped with a configuration button, you can add it to the network by pressing the configuration button on the device.
2. If the new device supports Wi-Fi Protected Setup and the connection way using PIN, you can add it to the network by entering the Device's PIN.

Note:

To build a successful connection by QSS, you should also do the corresponding configuration on a wireless adapter for QSS function meanwhile.

For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 5-5, and then the following screen will appear.

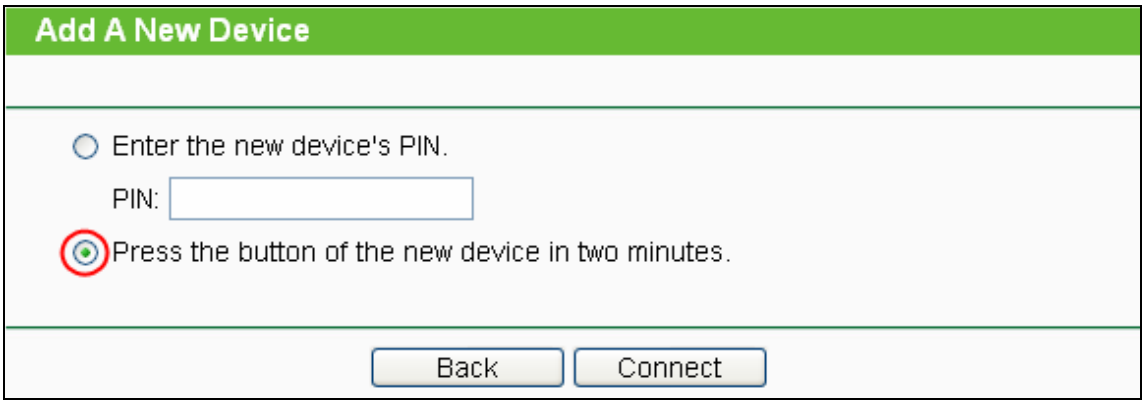


Figure 5-6 Add A New Device

Step 2: Choose "**Press the button of the new device in two minutes**" and click **Connect**.

Step 3: Configure the wireless adapter for QSS function by choosing "**Push the button on my access point**" in the QSS configuration utility as below, and then click **Next**.

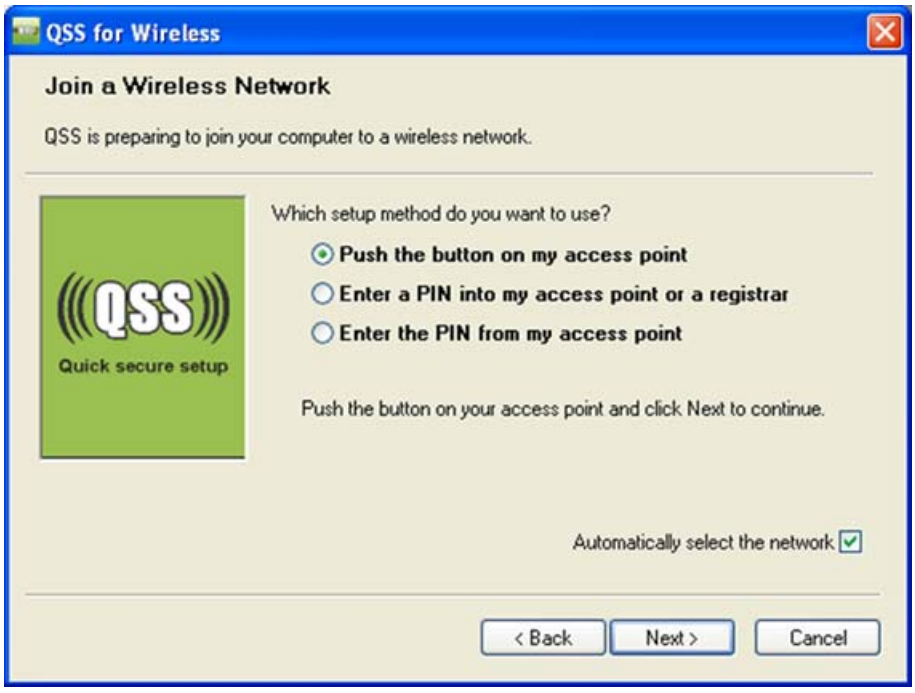


Figure 5-7 The QSS Configuration Screen of Wireless Adapter

Step 4: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.

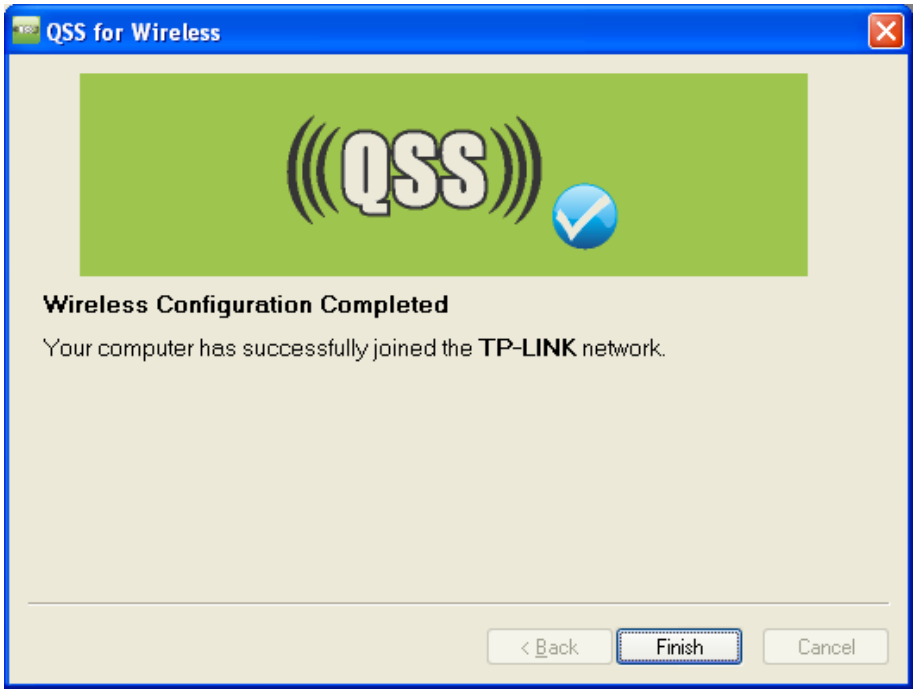


Figure 5-8 The QSS Configuration Screen of Wireless Adapter

II. By PIN

If the device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN in the following two methods.

Method One: Enter the PIN into my AP

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 5-5, and then the following screen will appear.

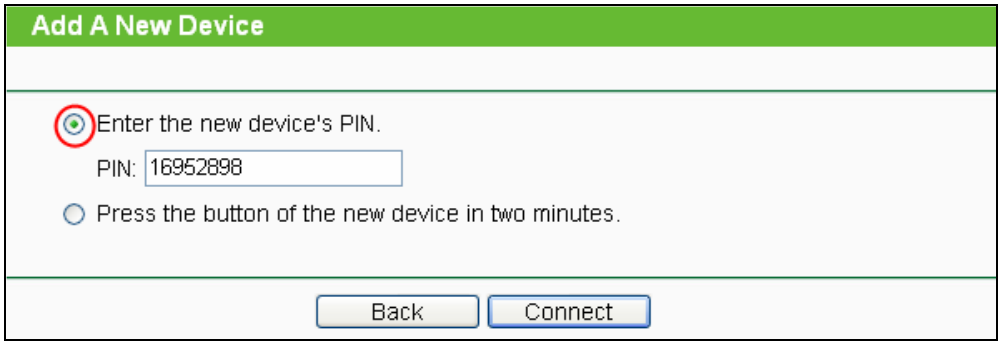


Figure 5-9 Add A New Device

Step 2: Choose "**Enter the new device's PIN**" and enter the PIN code （take 16952898 for example）of the wireless adapter in the field after **PIN** as shown in the figure above. Then click **Connect.**

☞ **Note:**

The PIN code of the adapter is always displayed on the QSS configuration screen as shown in Figure 5-10.

Step 3: Configure the wireless adapter for QSS function by choosing "**Enter a PIN into my access point or a registrar**" in the configuration utility of the QSS as below, and click **Next**.

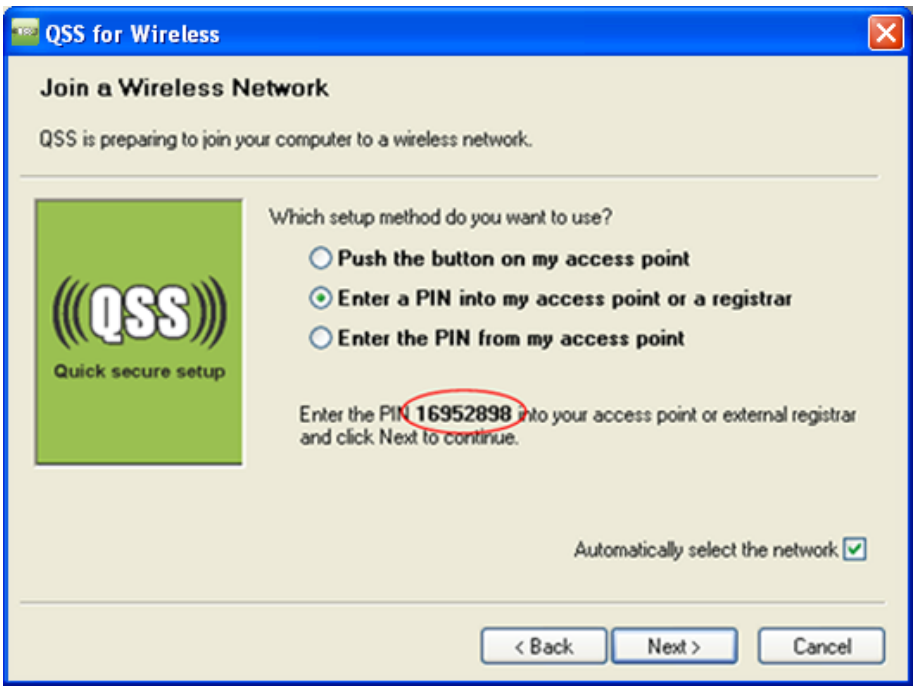


Figure 5-10 The QSS Configuration Screen of Wireless Adapter

Note:

In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

Method Two: Enter the PIN from my AP.

Step 1: Get the Current PIN code of the AP in Figure 5-5 (each AP has its unique PIN code. Here takes the default PIN code 12345670 of this AP for example).

Step 2: Configure the wireless adapter for QSS function by choosing "**Enter a PIN from my access point**" in the configuration utility of the QSS as below, and enter the PIN code of the AP into the field after "**Access Point PIN**". Then click **Next**.

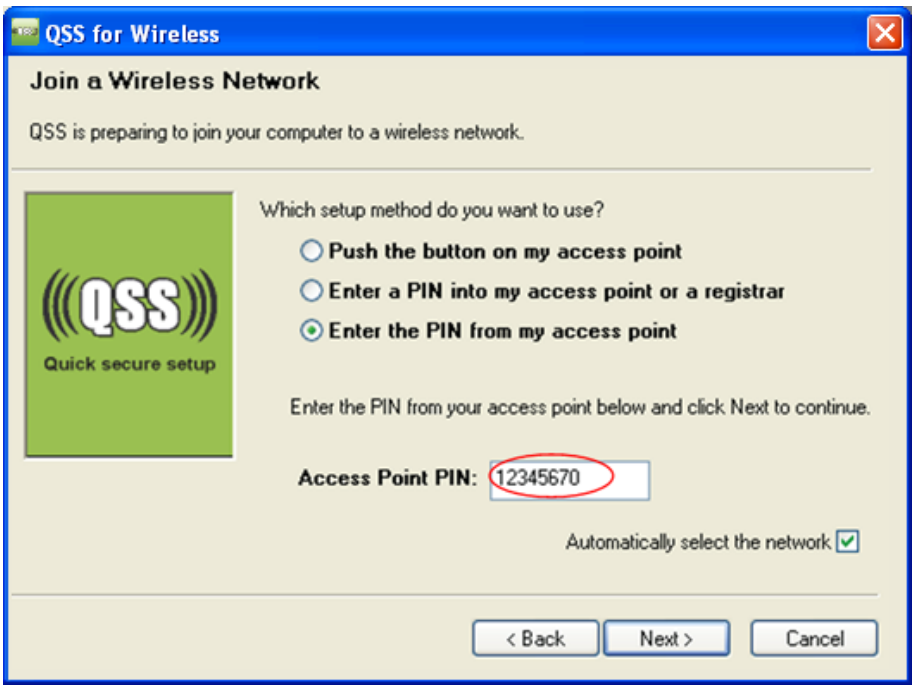


Figure 5-11 The QSS Configuration Screen of Wireless Adapter

Note:

The default PIN code of the AP can be found in its label or the QSS configuration screen as in Figure 5-5.

You will see the following screen when the new device has successfully connected to the network.

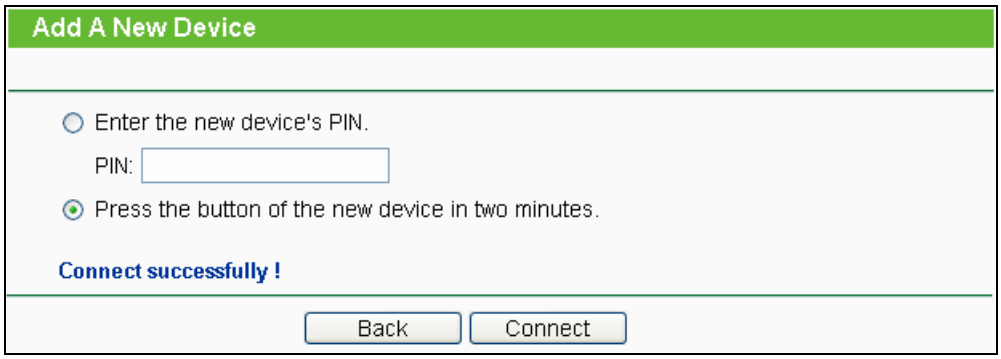


Figure 5-12

Note:

The QSS function cannot be configured if the Wireless function of the AP is disabled. Please make sure the Wireless function is enabled before configuring the QSS.

5.5 Operation Mode

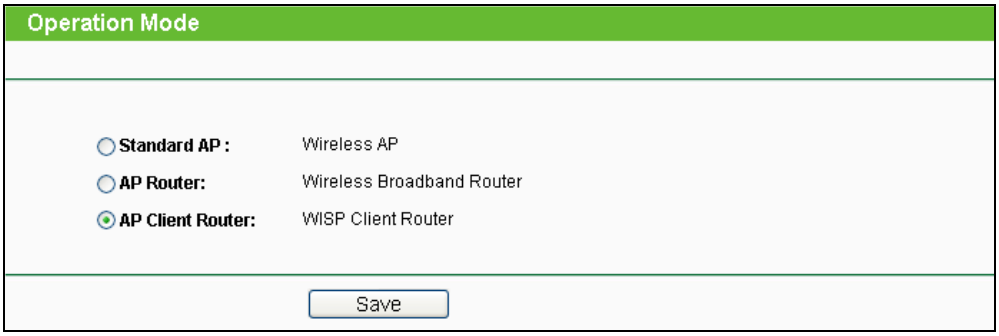


Figure 5-13

- **Standard AP**: In this mode, the device enables multi-users to accessing, and provides several wireless modes. Such as AP, Client, Repeater and so on.

- **AP Router**: In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.

- **AP Client Router**: In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at AP Client Router mode. The Ethernet port acts as a LAN port.

Be sure to click the **Save** button to save your settings on this page.

Note:

The Device will reboot automatically after you click the **Save** button.

5.6 Network

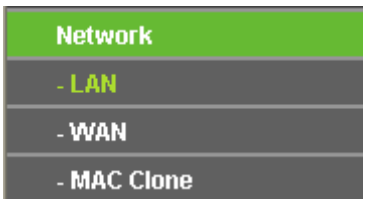


Figure 5-14 the Network Menu

There are three submenus under the Network menu (shown in Figure 5-14): **LAN, WAN** and **MAC Clone.** Click any of them, and you will be able to configure the corresponding function.

5.6.1 LAN

Choose menu "**Network** > **LAN**", and then you can configure the IP parameters of the LAN on the screen as below.

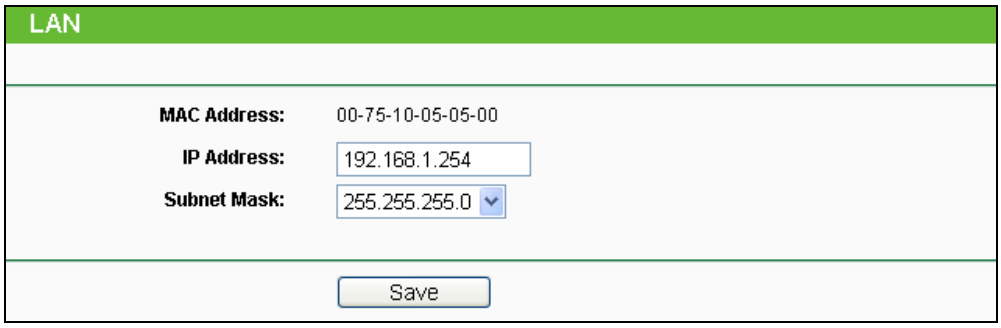


Figure 5-15 LAN

- **MAC Address** - The physical address of the LAN ports, as seen from the LAN. The value can not be changed.
- **IP Address** - Enter the IP address of your Device in dotted-decimal notation (factory default 192.168.1.254).
- **Subnet Mask** - An address code that determines the size of the network. Usually it is 255.255.255.0.

☞ **Note:**

1. If you change the LAN IP address, you must use the new IP address to login to the Device.
2. If the new LAN IP address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

5.6.2 WAN

Choose menu "**Network** > **WAN**", and then you can configure the IP parameters of the WAN on the screen below.

☞ **Note:**

There are five WAN connection types in AP Client Router mode: Dynamic IP, Static IP, PPPoE, L2TP, and PPTP; while there is one more type in AP Router mode, **BigPond Cable**.

1. If your ISP is running a DHCP server, select the **Dynamic IP** option. Then the Device will automatically get IP parameters from your ISP. You can see the page as follow (Figure 5-16).

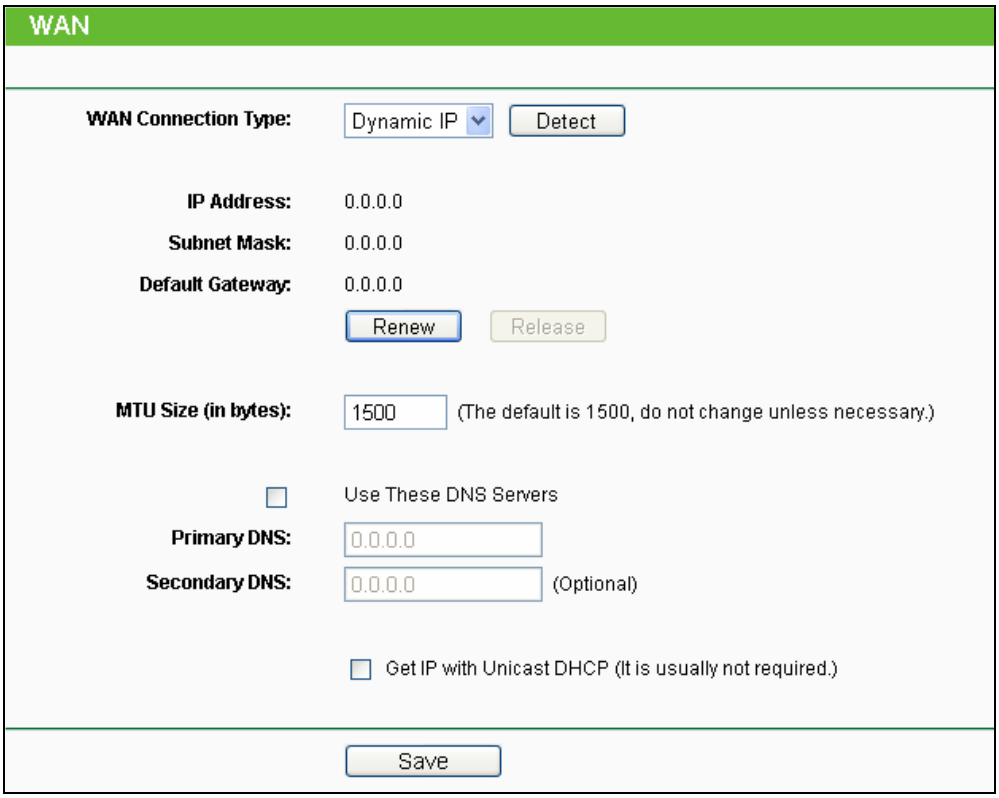


Figure 5-16 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc.

- **IP Address -** The IP address assigned by your ISP dynamically.
- **Subnet Mask -** The subnet mask assigned by your ISP dynamically.
- **Default Gateway -** The default gateway assigned dynamically by your ISP.
- **MTU Size (in bytes) -** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS IP addresses, select **Use These DNS Servers** and enter the **Primary DNS** and **Secondary DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- **Primary DNS -** Enter the DNS IP address in dotted-decimal notation provided by your ISP.
- **Secondary DNS -** Enter another DNS IP address in dotted-decimal notation provided by your ISP.

Click the **Renew** button to renew the IP parameters from your ISP.

Click the **Release** button to release the IP parameters.

Note:

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- **Get IP with Unicast DHCP -** A few ISPs' DHCP servers do not support the broadcast applications. If you can't get the IP Address normally, you can choose Unicast. You generally need not to check this option.

Click the **Save** button to save your settings.

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select the **Static IP** option. The **Static IP** settings page will appear as shown in Figure 5-17.

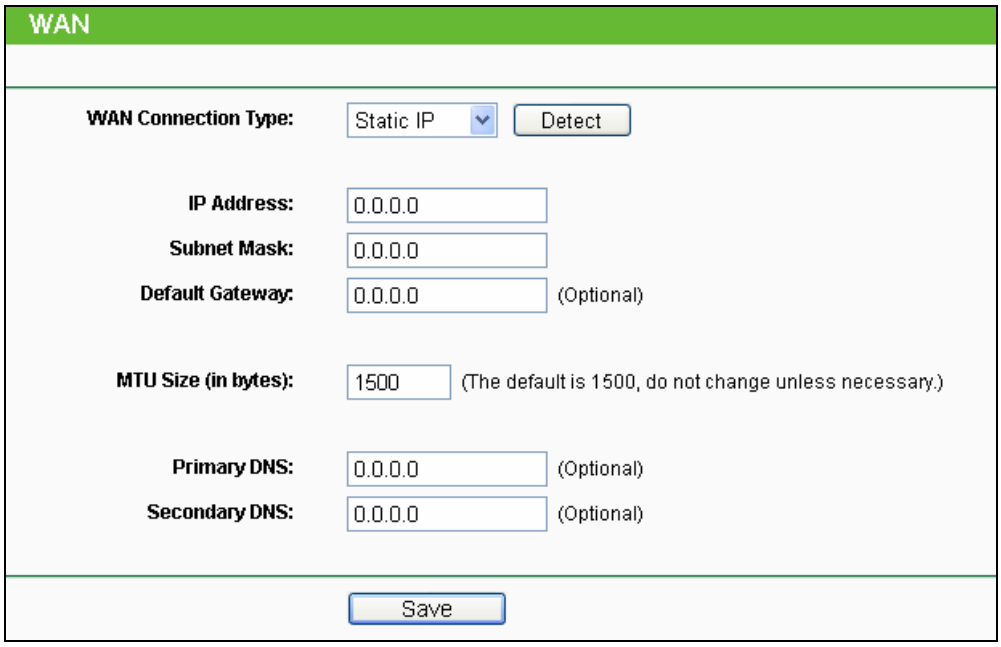


Figure 5-17 WAN - Static IP

Click the **Save** button to save your settings.

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. Then you should enter the following parameters (Figure 5-18):

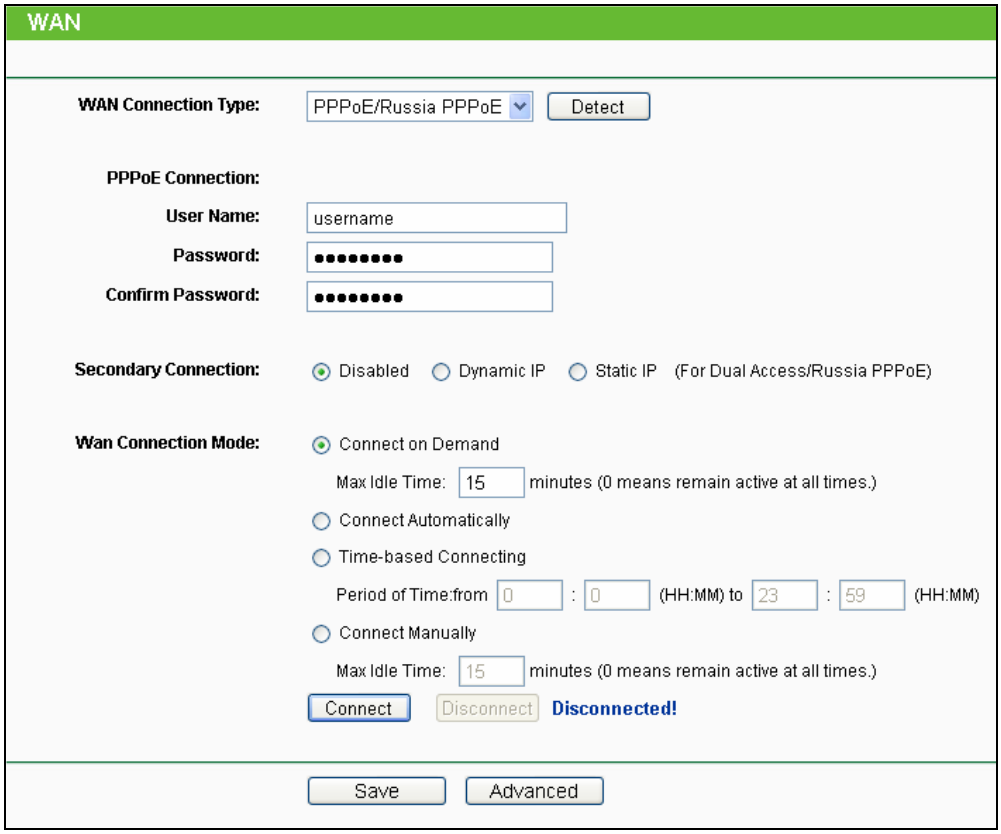


Figure 5-18 WAN – PPPoE/Russia PPPoE

➢ **PPPoE Connection**

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

➢ **Secondary Connection -** It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.

- **Disabled -** The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
- **Dynamic IP -** Use dynamic IP address to connect to the local area network provided by ISP.
- **Static IP -** Use static IP address to connect to the local area network provided by ISP.

➢ **WAN Connection Mode**

- **Connect on Demand -** You can configure the Device to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Device to automatically re-establish your connection when you attempt to access the Internet again. If you wish to activate **Connect on Demand**, put a check mark in the circle. If you want your Internet connection to remain active all the time, enter **0** in the **Max Idle Time** field.

Note:

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** (0~99 mins) because some applications visit the Internet continually in the background.

- **Connect Automatically -** Connect automatically after the Device is disconnected. To use this option, click the radio button.
- **Time-based Connecting -** You can configure the Device to make it connect or disconnect based on time. Enter the start time in HH-MM for connecting and end time in HH-MM for disconnecting in the **Period of Time** fields.
- **Connect Manually -** You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Device will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active all the times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Note:

1. Sometimes the connection cannot be disconnected although you specify a **Max Idle Time** (0~99 mins) because some applications visit the Internet continually in the background.
2. Only when you have set the system time on **System Tools -> Time Settings** page, the **Time-based Connecting** function can take effect.

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

Click the **Advanced** button to set up the advanced options.

Click the **Save** button to save your settings.

➢ If you want to do some advanced configurations, please click the **Advanced** button, and then the page shown in Figure 5-19 will appear.

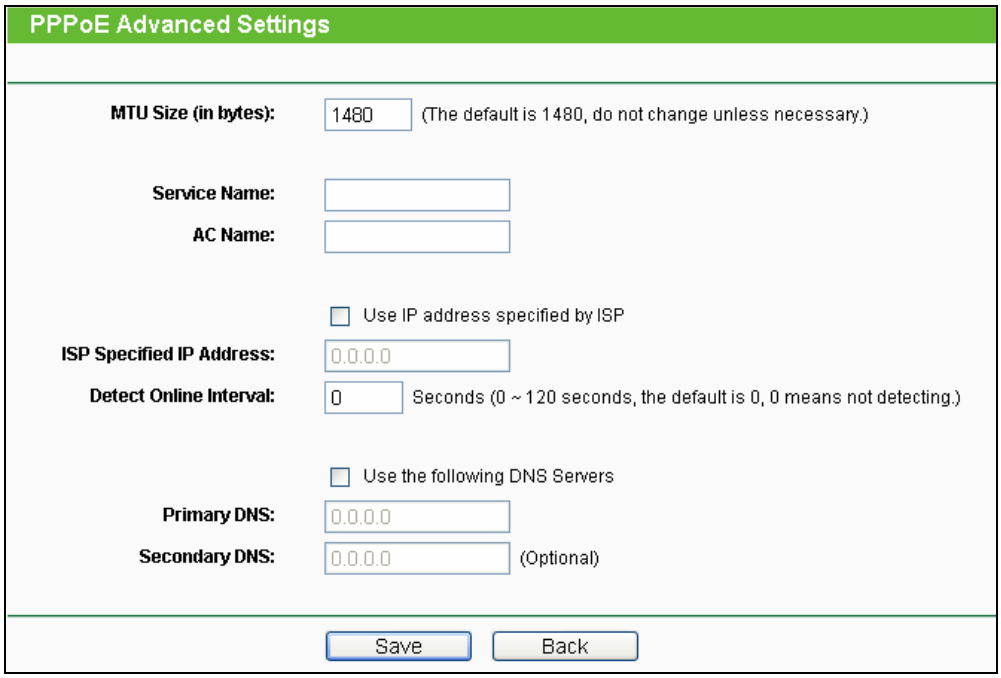


Figure 5-19 PPPoE Advanced Settings

- **MTU Size -** The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name -** They should not be done unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address** - If you know that your ISP does not automatically transmit IP address to the Device during login, click "**Use the IP Address specified by ISP**" checkbutton and enter the IP address in dotted-decimal notation, which is provided by your ISP.
- **Detect Online Interval** - The default value is 0. You can input the value between 0 and 120. The Device will detect Access Concentrator online every interval seconds. If the value is 0, it means not detecting.
- **Use the following DNS Servers** - If your ISP specifies a DNS server IP address for you, click the checkbox, and fill the **Primary DNS** and **Secondary DNS** blanks below. The **Secondary DNS** is optional. Otherwise, the DNS servers will be assigned dynamically from ISP.
- **Primary DNS** - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - (Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.

☞ **Note:**

The new advanced PPPoE parameters will not take effect until you dial-up again.

Click the **Save** button to save your settings.

Click the **Back** button when finished.

4. If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option. Then you should enter the following parameters in Figure 5-20.

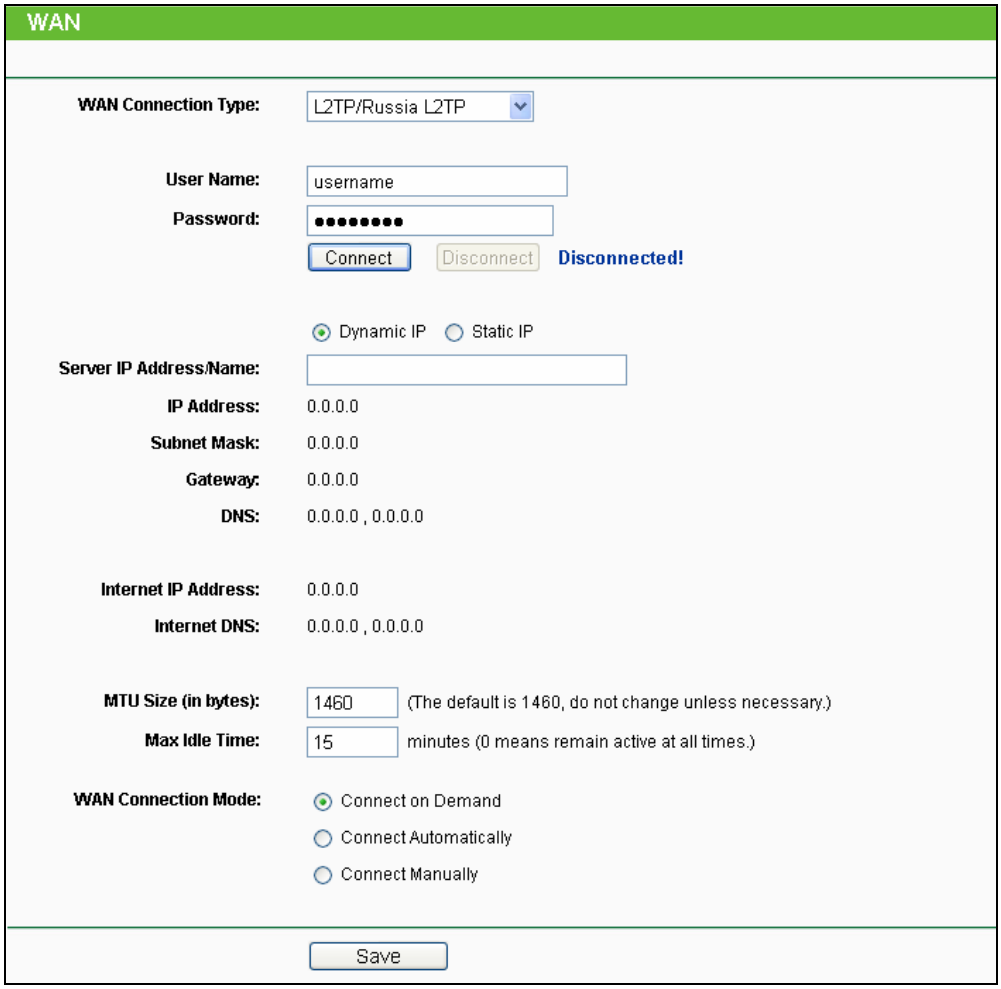


Figure 5-20 WAN – L2TP/Russia L2TP

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP -** Choose either one as you are given by your ISP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Connect on Demand -** You can configure the Device to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Device to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all time, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically -** Connect automatically after the Device is disconnected. To use this option, check the radio button.

- **Connect Manually -** You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Device will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, check the radio button. If you want your Internet connection to remain active at all time, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.

Note:

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time**, because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

5. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 5-21):

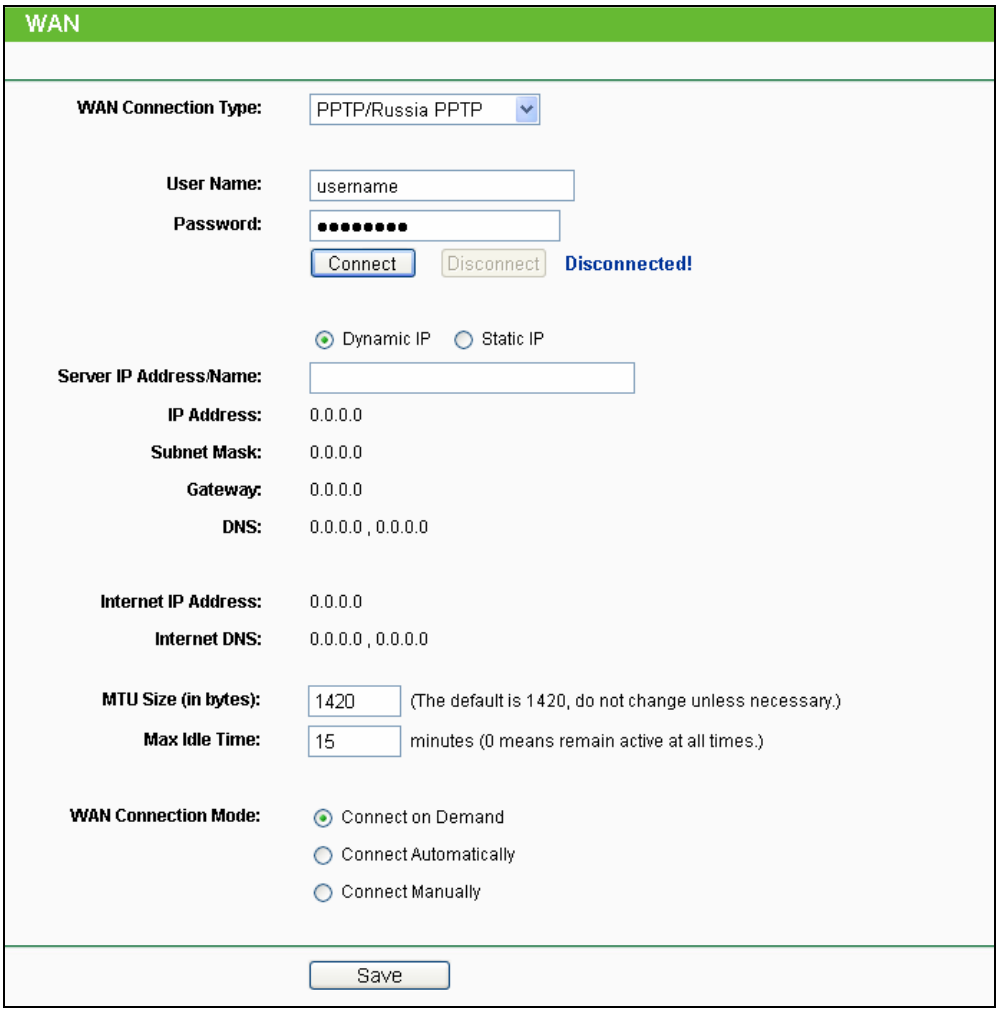


Figure 5-21 WAN – PPTP/Russia PPTP

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP -** Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.
 - If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.
 - Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Connect on Demand -** You can configure the Device to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Device to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically -** Connect automatically after the Device is disconnected. To use this option, check the radio button.
- **Connect Manually -** You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Device will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

☞ **Note:**

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

6. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable** option. And then you should enter the following parameters as in Figure 5-22.

☞ **Note:**

This type of WAN Connection is only available in AP Router mode, but not in AP Client Router Mode.

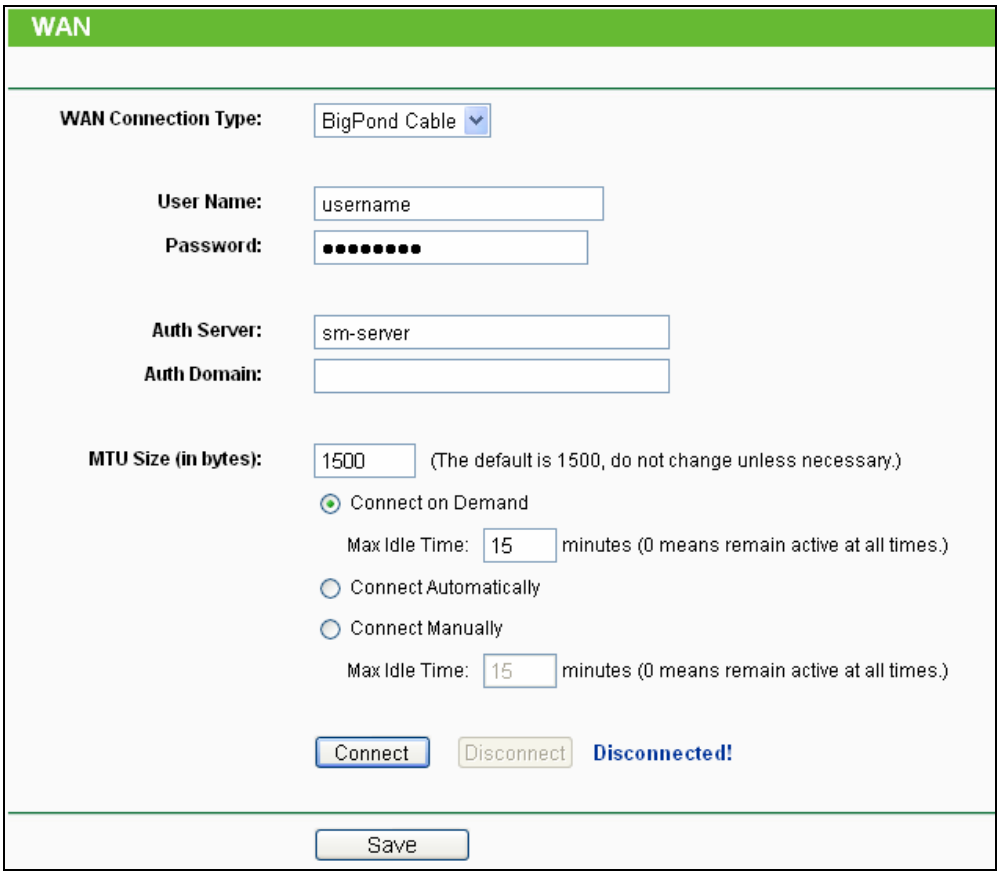


Figure 5-22 WAN – BigPond Cable

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server -** Enter the authenticating server IP address or host name.
- **Auth Domain -** Type in the domain suffix server name based on your location.

 NSW / ACT - **nsw.bigpond.net.au**
 VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
 QLD - **qld.bigpond.net.au**

- **MTU Size -** The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Connect on Demand -** In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter “0” in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically -** The connection can be re-established automatically when it was down.

- **Connect Manually -** You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.
- Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

☞ **Note:**

Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

5.6.3 MAC Clone

Choose menu "**Network > MAC Clone**", and then you can configure the **WAN MAC Address** on the screen below, as shown in Figure 5-23:

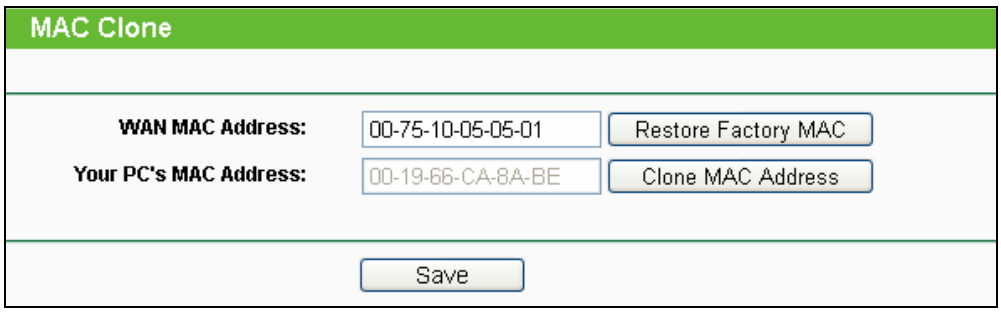


Figure 5-23 MAC Address Clone

- **WAN MAC Address -** This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address of your adapter, please enter the correct MAC address into this field. Usually, you do not need to change anything here. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address -** This field displays the MAC address of the PC that is managing the Device. If the MAC address of your adapter is registered, you can click the **Clone MAC Address** button, and then it will be filled into the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

☞ **Note:**

1. Only the PC(s) in your LAN can use the **MAC Address Clone** feature.
2. If you change **WAN MAC Address** when the WAN connection type is PPPoE, it will not take effect until the connection is re-established.

5.7 Wireless

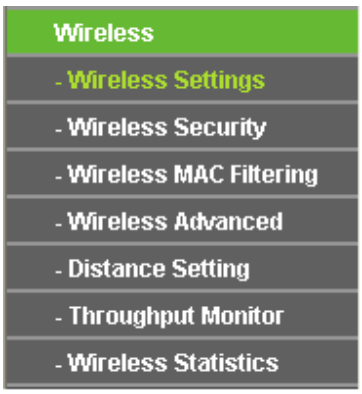


Figure 5-24 Wireless menu in AP Router Mode

In AP Router mode, there are seven submenus under the Wireless menu (shown in Figure 5-24): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced**, **Distance Setting**, **Throughput Monitor** and **Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function.

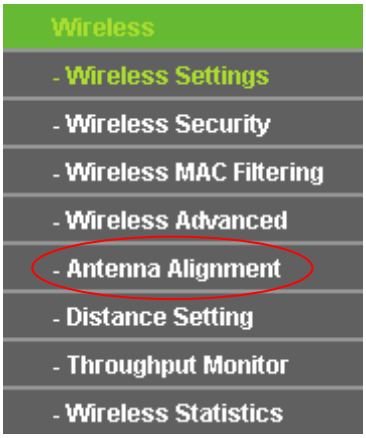


Figure 5-25 Wireless menu in AP Client Router Mode

In AP Client Router mode, there are eight submenus under the Wireless menu (shown in Figure 5-25): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced**, **Antenna Alignment, Distance Setting**, **Throughput Monitor** and **Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function.

☞ **Note:**

Notably, there is one more submenu in AP Client Router mode, which is **Antenna Alignment**.

5.7.1 Wireless Settings

Choose menu "**Wireless > Wireless Settings**", and then you can configure the basic settings for the wireless network on the **Wireless Settings** page（Figure 5-26 & Figure 5-27）.

Note:

There are differences between the Wireless Settings page in AP Router mode and that in AP Client Router mode, as shown in Figure 5-26 & Figure 5-27.

1. Wireless settings in AP Router mode

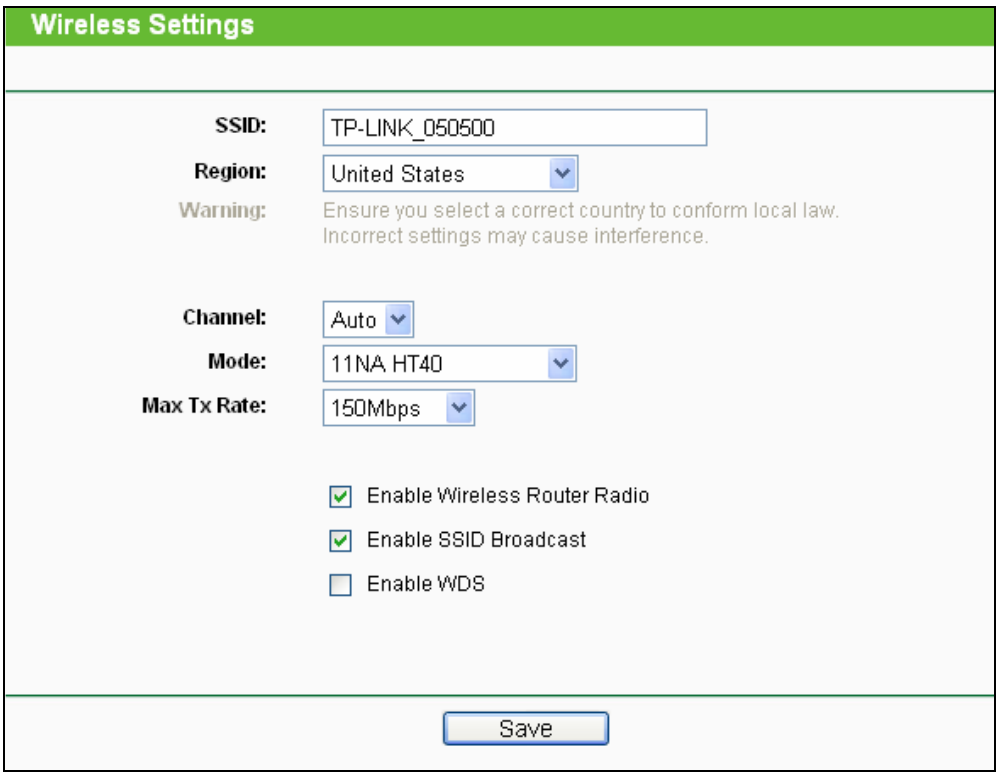


Figure 5-26 Wireless Settings in AP Router mode

- **Wireless Radio**- Enable or disable the wireless radio.
- **SSID**- Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **TP-LINK_xxxxxx** (xxxxxx indicates the last unique six characters of each Device's MAC address), which can ensure your wireless network security. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySsid**.
- **Region**- Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- **Channel**- This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the Device will select the best channel automatically.
- **Mode**- This field determines the wireless mode which the Device works on.
- **Max Tx Rate**- You can limit the maximum tx rate of the Device through this field. You can select one of security options listed as the below items.

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Device without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.
 For **ASCII**, the length should be between 8 and 63 characters.
 For **Hexadecimal**, the length should be between 8 and 64 characters.
 Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

2. Wireless settings in AP Client Router mode

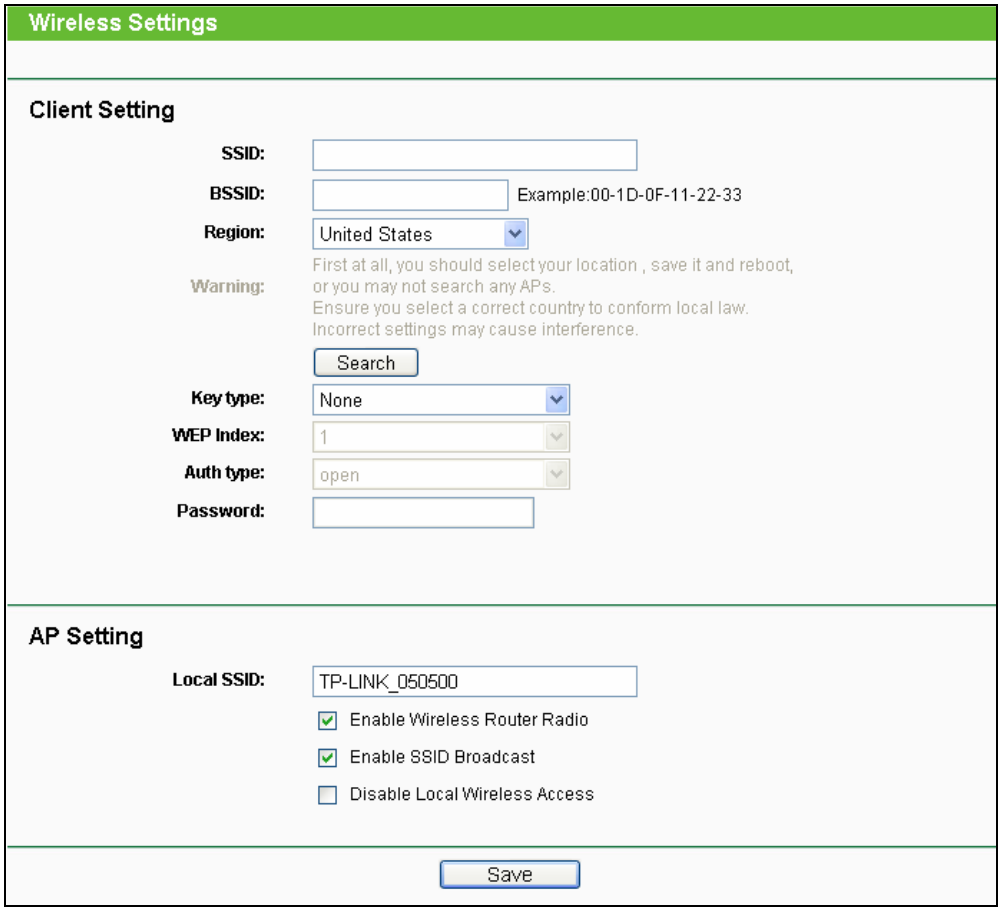


Figure 5-27 Wireless Settings in AP Client Router mode

- **SSID -** The SSID of the AP your Device is going to connect to as a client. You can also use the search function to select a SSID to join.
- **BSSID -** The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select a BSSID to join.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of

the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

- **Search -** Click this button, you can search the AP which runs in the current channel.
- **Key type -** This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- **WEP Index -** This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Auth Type -** This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization type of the Root AP.
- **Password -** If the AP your Device is going to connect needs password, you need to fill the password in this blank.
- **Local SSID -** Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Enable Wireless Router Radio -** The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
- **Enable SSID Broadcast -** If you select the **Enable SSID Broadcast** checkbox, the wireless Router will broadcast its name (SSID) on the air.
- **Disable Local Wireless Access -** If you select the **Disable Local Wireless Access** checkbox, the wireless Device will disable local wireless access; other stations will not be able to access the Device by wireless.

Click **Search** button on the Wireless page shown as Figure 5-27, and then AP List page will appear, as shown in Figure 5-28. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the desired item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 5-29.

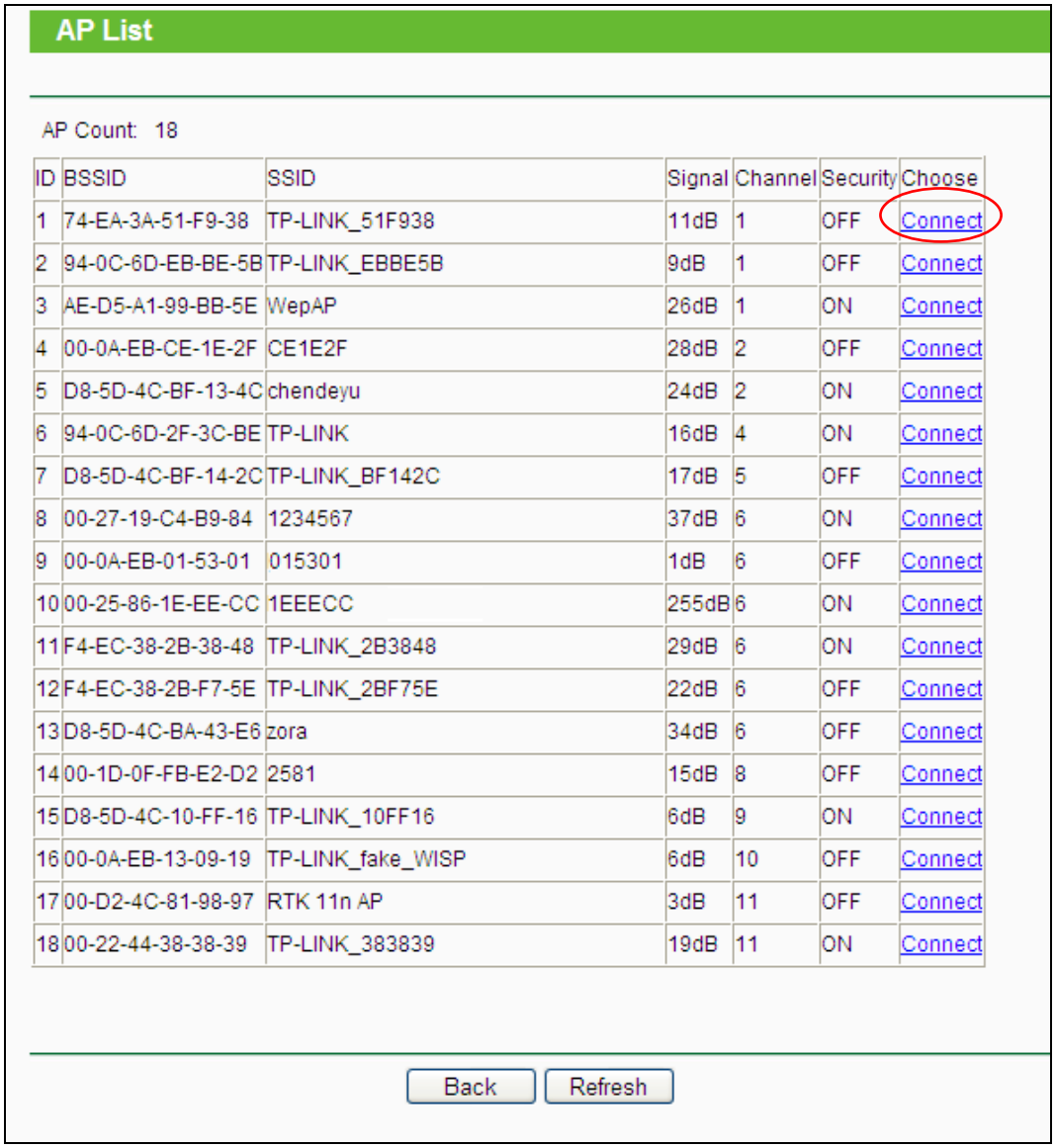


Figure 5-28 AP List

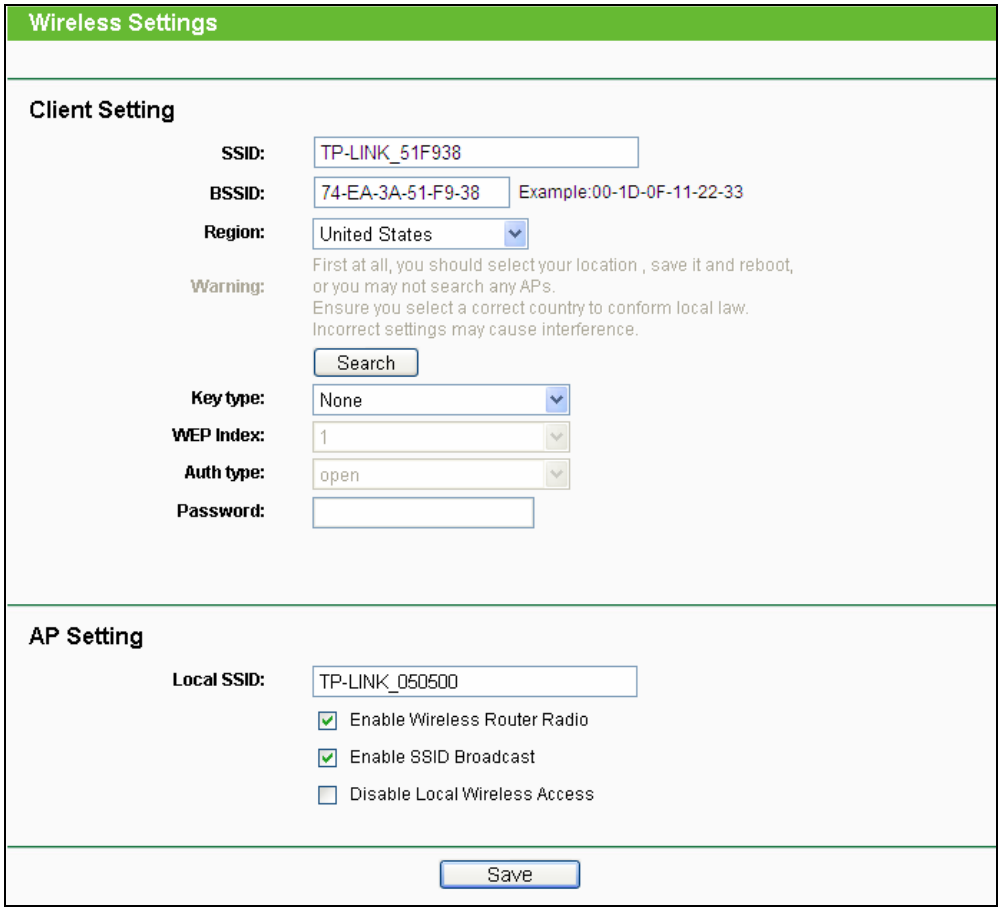


Figure 5-29

Note:

If you know the SSID of the desired AP, you can also input it to the field "SSID" manually.

Be sure to click the **Save** button to save your settings on this page.

Note:

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device:

- Near the center of the area in which your wireless stations will operate;
- In an elevated location such as a high shelf;
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones;
- With the Antenna in the upright position;
- Away from large metal surfaces.

Note:

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

5.7.2 Wireless Security

Choose menu "**Wireless > Wireless Security**", and then you can configure the security settings of your wireless network.

There are three wireless security modes supported by the Device: **WEP** (Wired Equivalent Privacy), **WPA/WPA2** (Wi-Fi Protected Access/ Wi-Fi Protected Access 2), and **WPA-PSK/WPA2-PSK** (Pre-Shared Key).

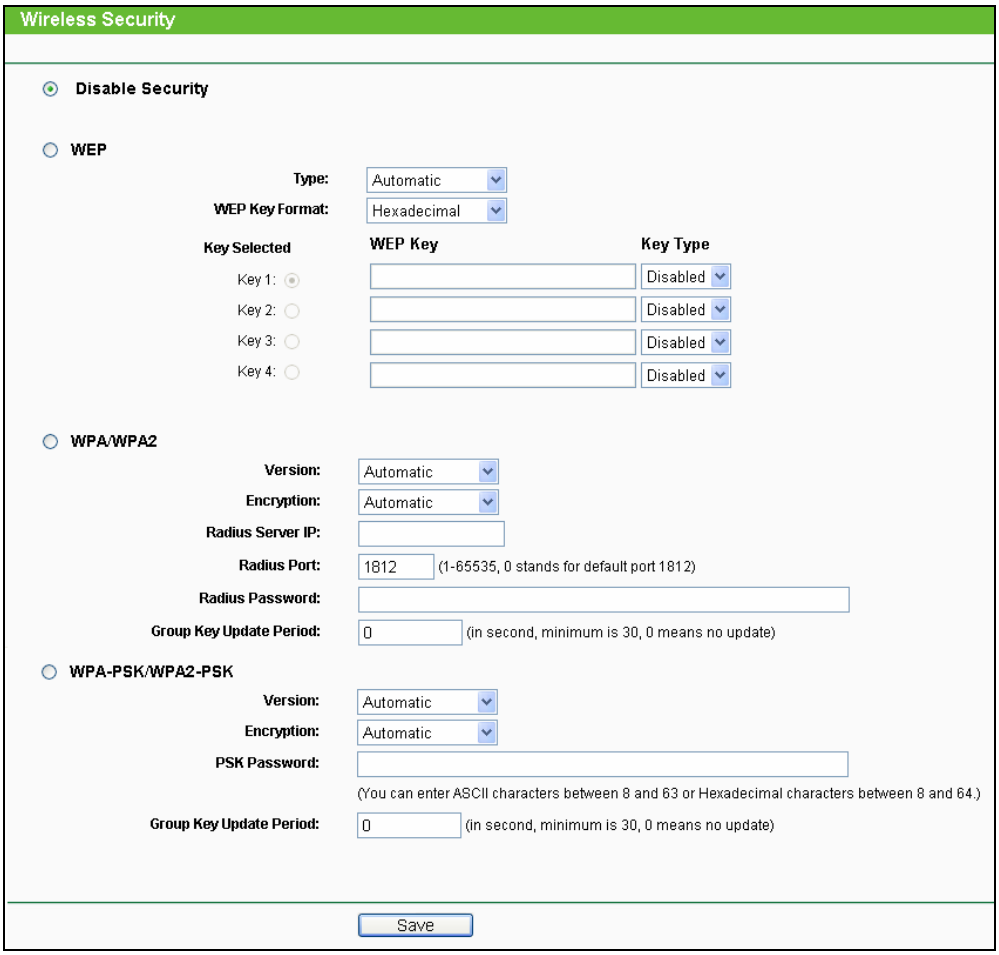


Figure 5-30 Wireless Security

Note:

Only in Standard AP mode, the current operation mode is shown at the top. Besides, if Multi-SSID, a sub mode of Standard AP, is selected, you can choose one of the 4 SSIDs from the pull-down list.

You can select one of the following security options:

- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.

- **WEP -** Select 802.11 WEP security.
- **WPA-PSK -** Select WPA based on pre-shared passphrase.
- **WPA -** Select WPA based on Radius Server.

Each security option has its own settings as described follows:

- **WEP**

- **Type -** You can select one of following types:

 Automatic - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

 Shared Key - Select 802.11 Shared Key authentication.

 Open System - Select 802.11 Open System authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

- **WEP Key settings** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.

- **Key Type -** You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid.

 For 64-bit encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters.

 For 128-bit encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters.

 For 152-bit encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

Note:

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

- **WPA/WPA2**

- **Version -** You can select one of following versions:

 Automatic - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.

WPA - Wi-Fi Protected Access.

WPA2 - WPA version 2.

- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.
- **Radius Server IP -** Enter the IP address of the Radius Server.
- **Radius Port -** Enter the port that radius service uses.
- **Radius Password -** Enter the password for the Radius Server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

➢ **WPA-PSK/WPA2-PSK**

- **Version -** You can select one of following versions:

 Automatic - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

 WPA-PSK - Pre-shared key of WPA

 WPA2-PSK - Pre-shared key of WPA2

- **Encryption -** You can select either **Automatic**, or **TKIP** or **AES**.
- **PSK Password -** You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

5.7.3 Wireless MAC Filtering

Choose menu "**Wireless > MAC Filtering**", and then you can control the wireless access by configuring the **Wireless MAC Filtering** function, as shown in Figure 5-31.

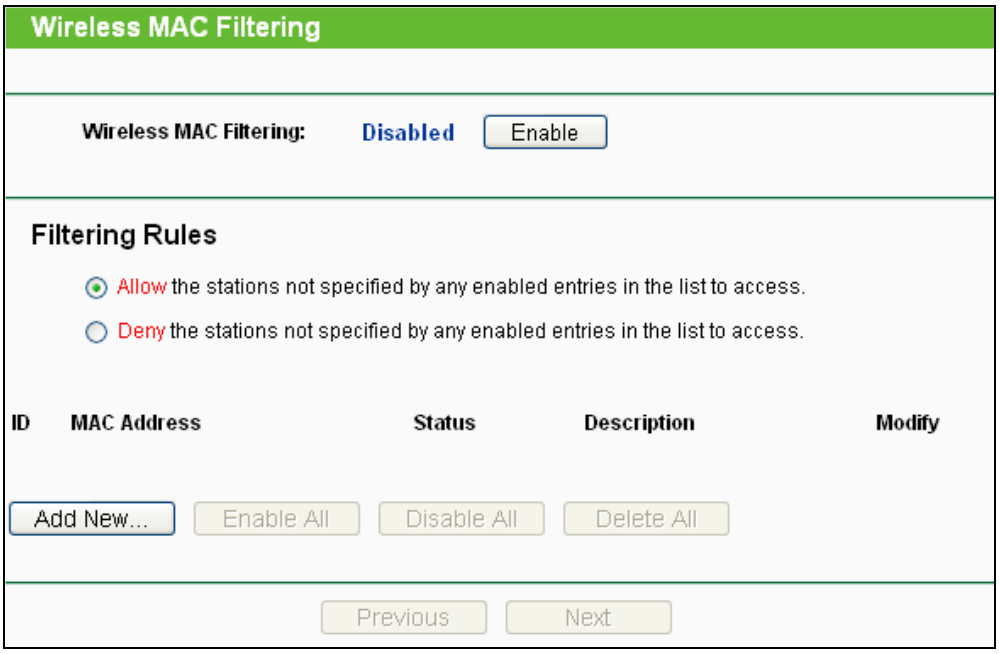


Figure 5-31 Wireless MAC Filtering

➢ To filter wireless users by MAC Address, click **Enable**. The default setting is **Disable**.

- **MAC Address -** The wireless station's MAC address that you want to filter.
- **Description -** A simple description of the wireless station.
- **Status -** The status of this entry, either **Enabled** or **Disabled**.

➢ To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 5-32:

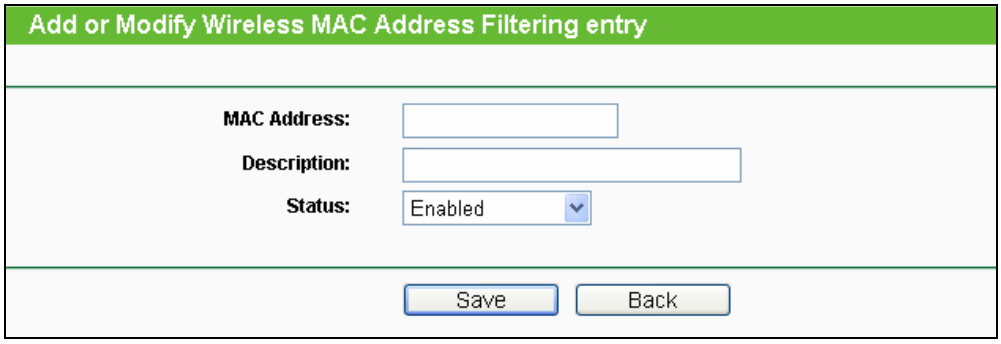


Figure 5-32 Add or Modify Wireless MAC Address Filtering entry

➢ **To add or modify a MAC Address Filtering entry, follow these instructions:**

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX(X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Give a simple description for the wireless station in the **Description** field. For example: Wireless station A.

3. Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

➢ **To modify or delete an existing entry:**

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page.

Click the **Previous** button to return to the previous page.

➢ **For example:** If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the Device, but all the other wireless stations cannot access the Device, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button "**Deny the stations not specified by any enabled entries in the list to access**" for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button.
 1) Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the **MAC Address** field.
 2) Enter wireless station A/B in the **Description** field.
 3) Select **Enabled** in the **Status** pull-down list.
 4) Click the **Save** button.
 5) Click the **Back** button.

The filtering rules that are configured should be similar to the following list:

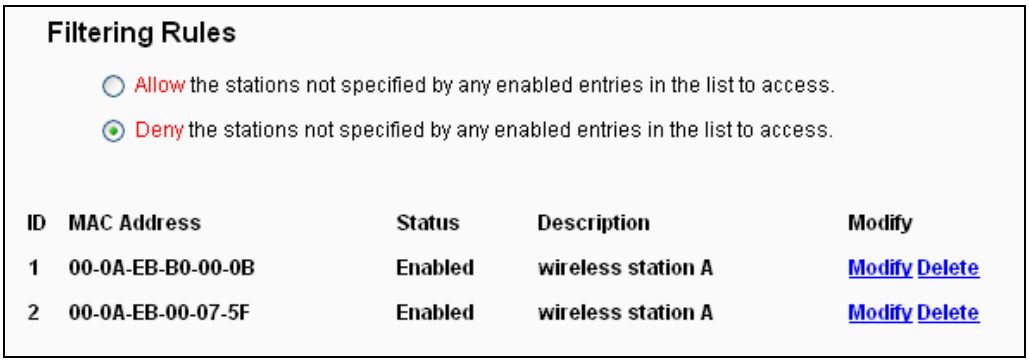


Figure 5-33

5.7.4 Wireless Advanced

Choose menu "**Wireless > Wireless Advanced**", and then you can configure the advanced settings of your wireless network.

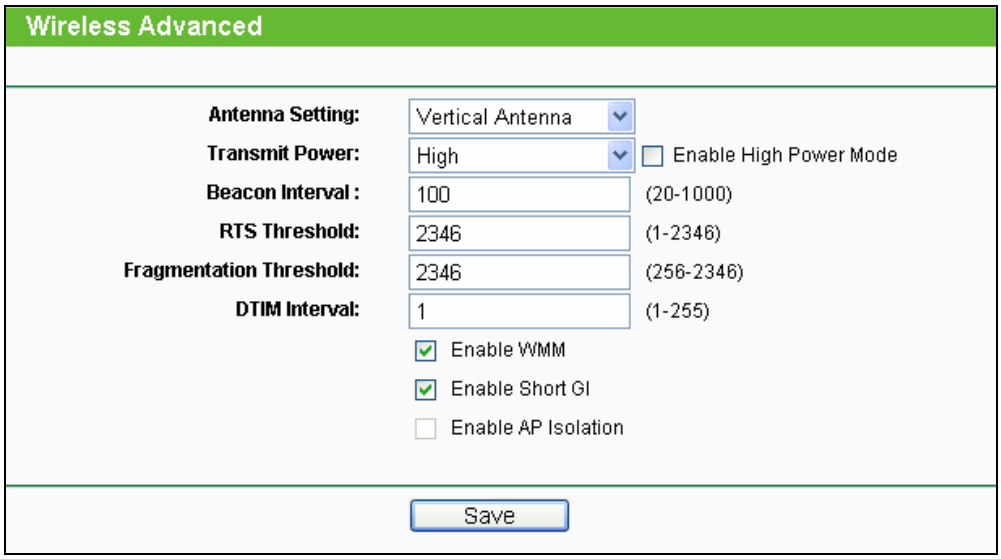


Figure 5-34 Wireless Advanced

- **Antenna Settings -** The polarization of an antenna. You can select Vertical Antenna, Horizontal Antenna, or External Antenna.
- **Transmit Power -** Here you can specify the transmit power of the Device. You can select High, Middle or Low whichever you would like. High is the default setting and is recommended.
- **Beacon Interval -** The beacons are the packets sent by the Device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 20-1000 milliseconds. The default value is 100.

- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM -** WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI -** This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation -** Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

☞ **Note:**

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise, it may result in lower wireless network performance.

5.7.5 Antenna Alignment

☞ **Note:**

This function is not available in AP Router mode, but in both Standard AP mode and AP Client Router mode.

Choose menu "**Wireless > Antenna Alignment**", and then you can know how remote the Device's signal strength changes while changing the antenna's direction.

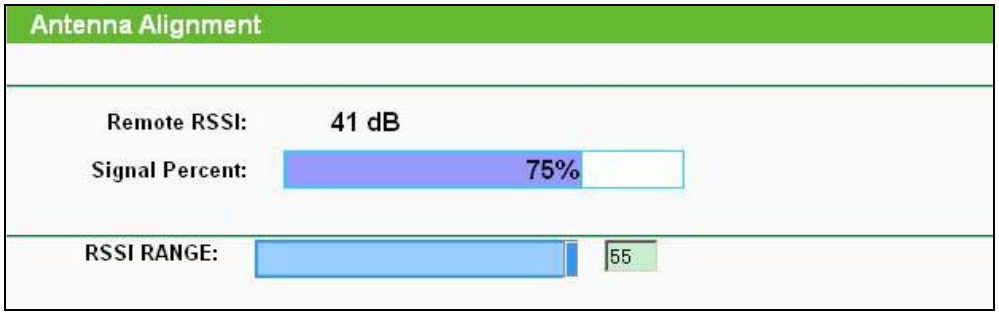


Figure 5-35 Antenna Alignment

- **Remote RSSI -** Remote AP's signal strength value.
- **Signal Percent -** The ratio of RSSI to RSSI RANGE in percentage.
- **RSSI RANGE -** You can drag the Slider to set or input the RSSI RANGE value.

Note:

It only works after you have established connection to remote AP in client mode.

5.7.6 Distance Settings

Choose menu "**Wireless > Distance Settings**", and then you can adjust the wireless range in outdoor conditions.

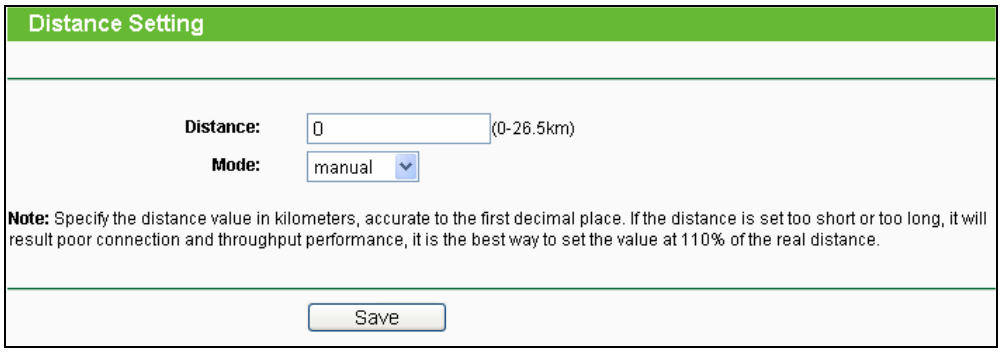


Figure 5-36

This is a critical feature required for stabilizing outdoor links. Enter the distance of your wireless link, and then the software will optimize the frame ACK timeout value automatically.

Note:

One hundred-meter is the smallest unit of this setting.

5.7.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in Figure 5-37.

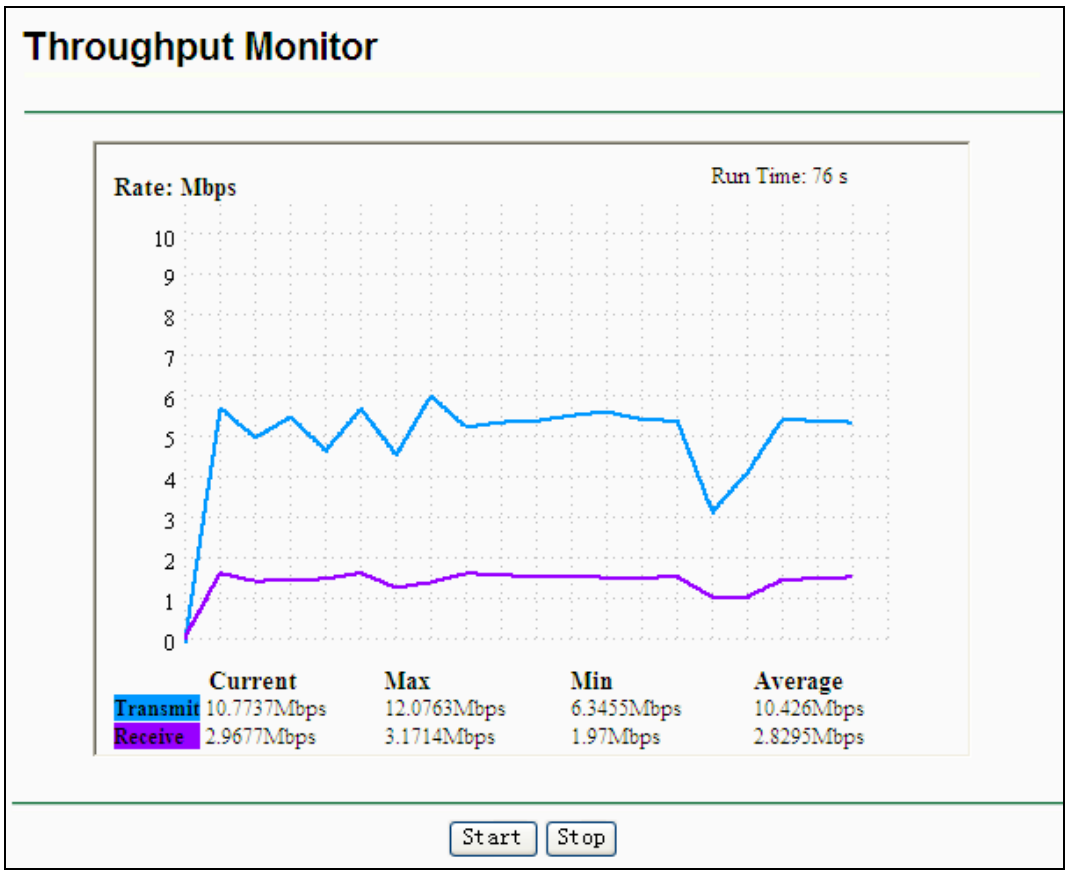


Figure 5-37 Throughput Monitor

- **Rate -** The Throughput unit.
- **Run Time -** How long this function is running.
- **Transmit -** Wireless transmit rate information.
- **Receive -** Wireless receive rate information.

Click the **Start** button to start wireless throughput monitor.

Click the **Stop** button to stop wireless throughput monitor.

5.7.8 Wireless Statistics

Choose menu "**Wireless > Wireless Statistics**", and then you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

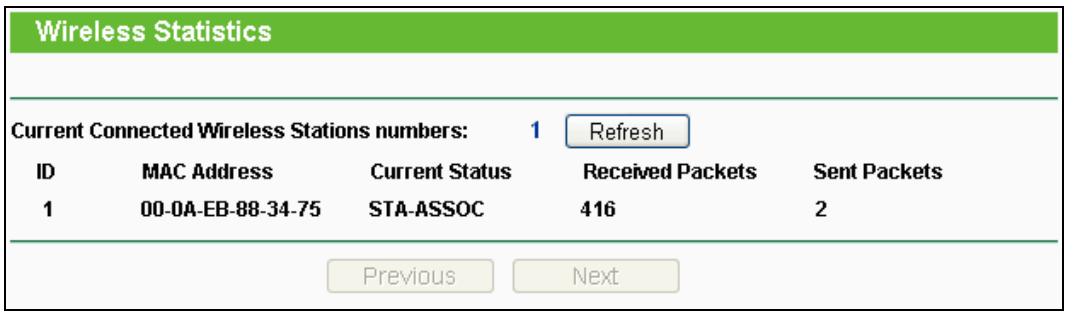


Figure 5-38 Wireless Statistics

- **MAC Address -** the connected wireless station's MAC address.
- **Current Status -** the connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected.
- **Received Packets -** packets received by the station.
- **Sent Packets -**packets sent by the station.
- **Belong To -** the SSID that station belong to.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

Note:

This page will be refreshed automatically every 5 seconds.

5.8 DHCP

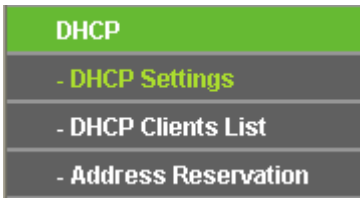


Figure 5-39 The DHCP menu

The DHCP (Dynamic Host Configuration Protocol) server function, which provides the TCP/IP configuration for all the PCs that are connected to the device in the LAN, is **Disable** by default.

There are three submenus under the DHCP menu (shown in Figure 5-39), **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

5.8.1 DHCP Settings

Choose menu "**DHCP > DHCP Settings**", and then you can configure the DHCP Server on the page as shown in Figure 5-40. The Device is set up by default as a DHCP server.

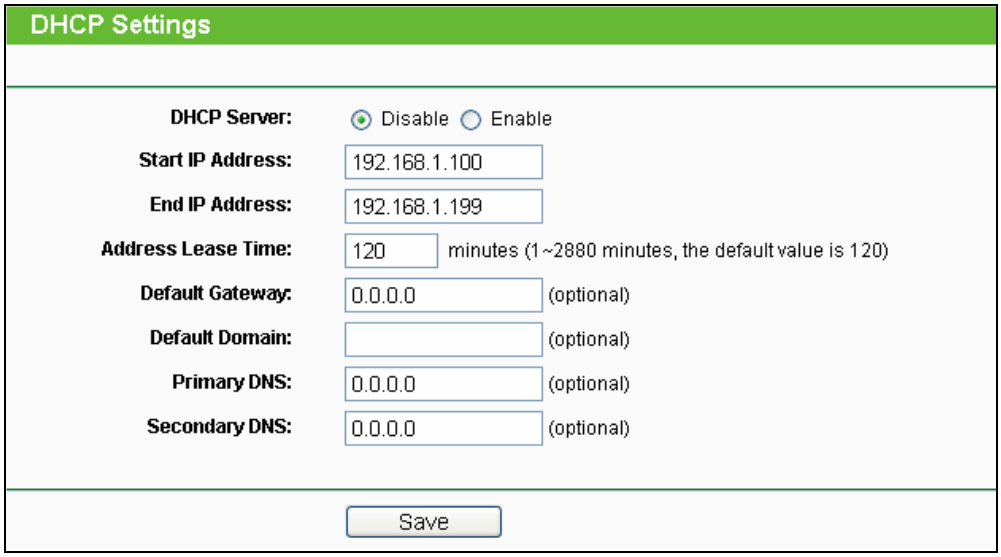


Figure 5-40 DHCP Settings

- **DHCP Server - Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network, or else you must configure the IP address of the computer manually.
- **Start IP Address -** This field specifies the first address in the IP Address pool. 192.168.1.100 is the default start IP address.
- **End IP Address -** This field specifies the last address in the IP Address pool. 192.168.1.199 is the default end IP address.
- **Address Lease Time –** It is the length of time a network user will be allowed to keep connecting to the device with the current DHCP Address. Enter the amount of time, in minutes, that the DHCP address will be "leased". The time range is 1~2880 minutes. The default value is 120 minutes.
- **Default Gateway -** (Optional) Input the IP Address of the gateway.
- **Default Domain -** (Optional) Input the domain name of your network.
- **Primary DNS -** (Optional) Input the DNS IP address provided by your ISP.
- **Secondary DNS -** (Optional) You can input the IP Address of another DNS server if your ISP provides two DNS servers.

Note:

To use the DHCP server function of the device, you should configure all computers in the LAN as "**Obtain an IP Address automatically**" mode. This function will take effect until the device reboots.

5.8.2 DHCP Clients List

Choose menu "**DHCP > DHCP Clients List**", and then you can view the information about the clients attached to the Device in the screen as shown in Figure 5-41.

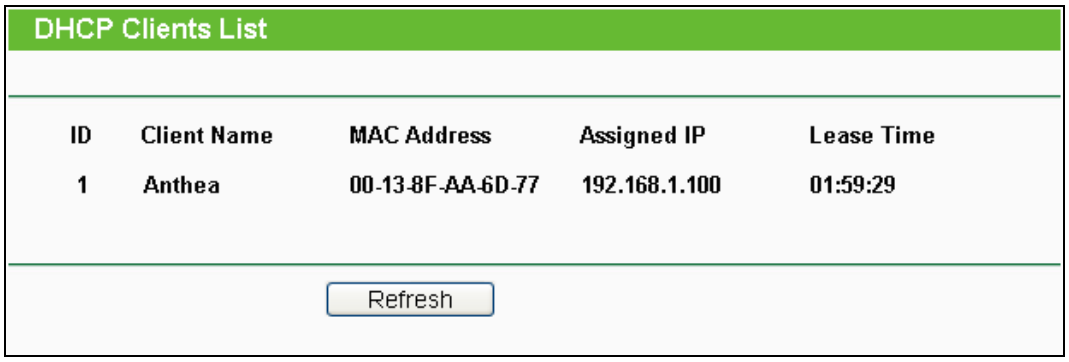


Figure 5-41 DHCP Clients List

- **Client Name -** The name of the DHCP client.
- **MAC Address -** The MAC address of the DHCP client.
- **Assigned IP -** The IP address that the device has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased.

You cannot change any of the values on this page.

To update this page and to show the current attached devices, click the **Refresh** button.

5.8.3 Address Reservation

Choose menu "**DHCP > Address Reservation**", and then you can view or add a reserved address for clients via the next screen (shown in Figure 5-42).

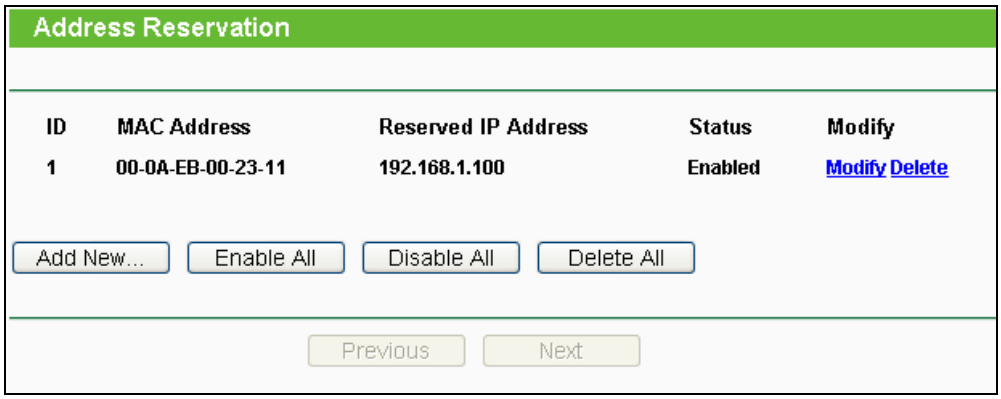


Figure 5-42 Address Reservation

When you specify a reserved IP address for a PC on the LAN, the PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

- **MAC Address** - The MAC Address of the PC that you want to reserve an IP address for.
- **Reserved IP Address** - The IP address that the device reserved.
- **Status** - It shows whether the entry is enabled or not.
- **Modify** - To modify or delete an existing entry.
- **To Reserve IP Addresses, you can follow these steps:**

1. Click **Add New…** button in Figure 5-42, then the **Add or Modify an Address Reservation Entry** page will appear as shown in Figure 5-43.
2. Enter the MAC Address (The format for the MAC Address is XX-XX-XX-XX-XX-XX) and the IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button.

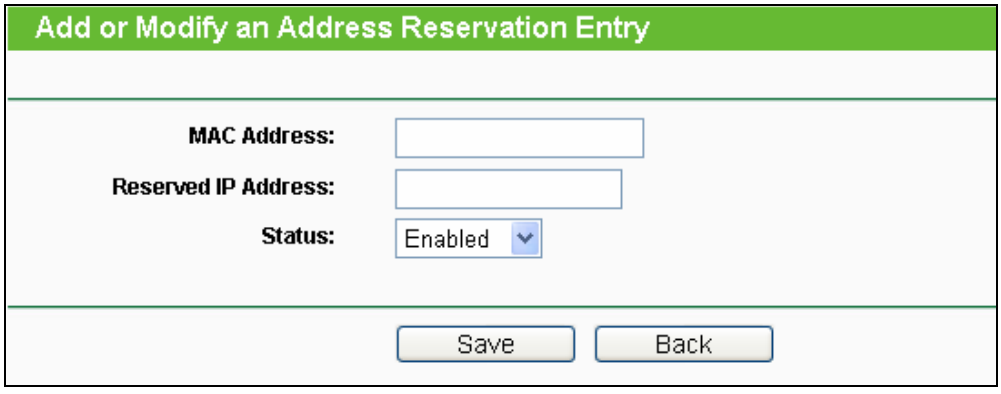


Figure 5-43 Add or Modify an Address Reservation Entry

➢ **To modify a Reserved IP Address, you can follow these steps:**

1. Select the reserved address entry as you desired, **Modify** it. If you wish to delete the entry, click the **Delete** link of the entry.
2. Click the **Save** button.

Click the **Add New...** button to add a new Address Reservation entry.

Click the **Enable All** button to enable all the entries in the table.

Click the **Disable All** button to disable all the entries in the table.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

5.9 Forwarding

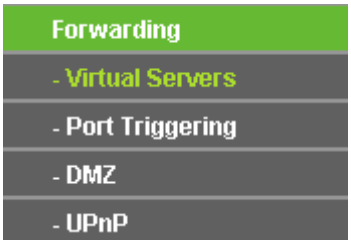


Figure 5-44 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 5-44): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

5.9.1 Virtual Servers

Choose menu "**Forwarding > Virtual Servers**", and then you can view and add virtual servers in the screen as shown in Figure 5-45.

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that is used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

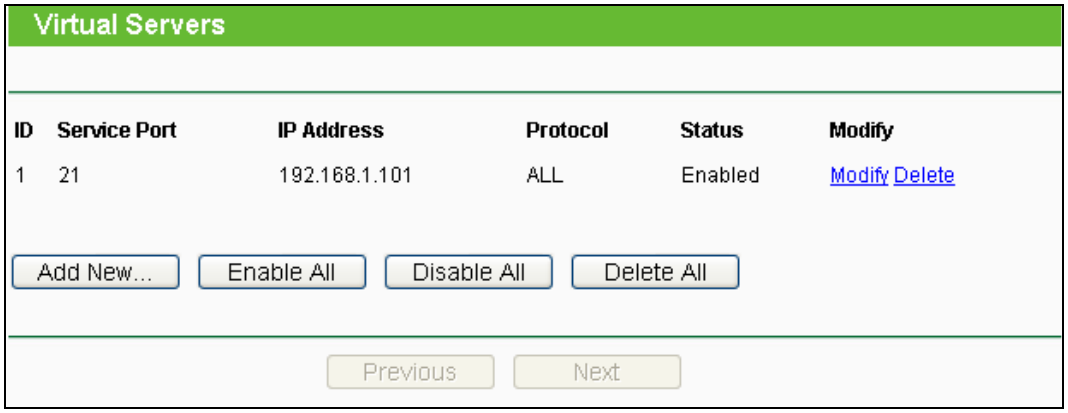


Figure 5-45 Virtual Servers

- **Service Port -** The numbers of External Ports. You can enter a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).
- **IP Address -** The IP address of the PC running the service application.
- **Protocol -** The protocol used for this application, either **TCP, UDP**, or **All** (all protocols are supported by the Device.).
- **Status -** The status of this entry. "Enabled" means the virtual server entry is enabled.
- **Common Service Port -** Some common services already exist in the pull-down list.
- **Modify -** To modify or delete an existing entry.
- **To setup a virtual server entry**, **you can follow these steps:**

1. Click the **Add New...** button.
2. Select the service you want to use from the **Common Service Port** list. If the **Common Service Port** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** box.
3. Enter the IP address of the computer running the service application in the **IP Address** box.
4. Select the protocol used for this application in the **Protocol** box: **TCP, UDP**, or **All**.
5. Select the **Enabled** option in the **Status** pull-down list.
6. Click the **Save** button.

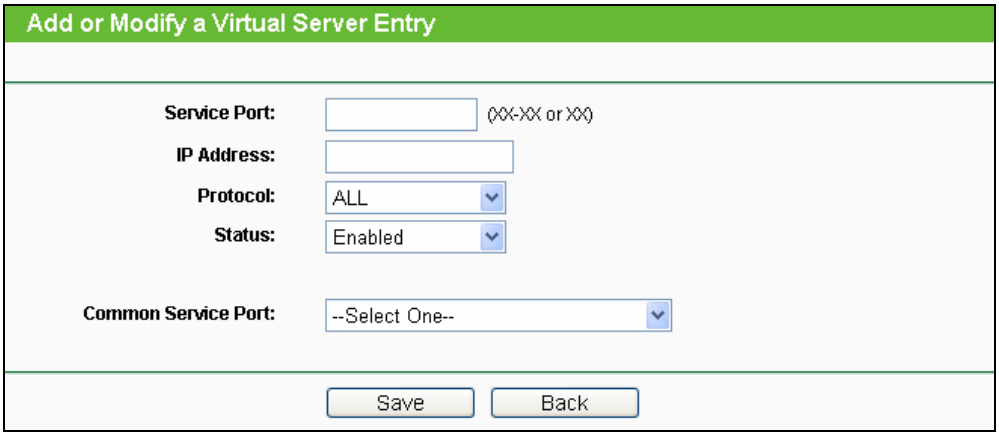


Figure 5-46 Add or Modify a Virtual Server Entry

Note:

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

➢ **To modify or delete an existing entry:**

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disabled All** button to make all entries enabled/disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

5.9.2 Port Triggering

Choose menu "**Forwarding > Port Triggering**", and then you can view and add port triggering in the screen as shown in Figure 5-47.

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

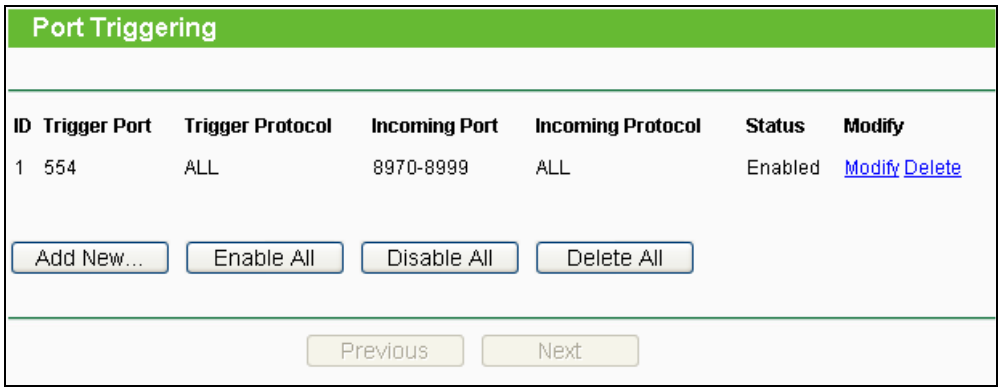


Figure 5-47 Port Triggering

➢ **Once configured, operation is as follows**:

1. A local host makes an outgoing connection to an external host using a destination port number defined in the **Trigger Port** field.
2. The Device records this connection, opens the incoming port or ports associated with this entry in the **Port Triggering** table, and associates them with the local host.
3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

➢ **Rules**:

- **Trigger Port -** The port for outgoing traffic. An outgoing connection using this port will Trigger this rule.
- **Trigger Protocol -** The protocol used for Trigger Ports, either **TCP, UDP**, or **All** (all protocols are supported by the Device.).
- **Incoming Port -** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",". For example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** The protocol used for Incoming Port, either TCP, UDP, or ALL (all protocols are supported by the Device.).
- **Status -** The status of this entry. Enabled means the Port Triggering entry is enabled.
- **Modify -** To modify or delete an existing entry.
- **Common Applications -** Some popular applications already listed in the from the pull-down list of Incoming Protocol.

➢ **To add a new rule do the following on the Port Triggering screen**:

1. Click the **Add New...** button.
2. Enter a port number used by the application to send an outgoing request in the Trigger Port box.
3. Select the protocol used for the **Trigger Port** from the pull-down list of Trigger Protocol, either TCP, UDP, or All.
4. Enter the range of port numbers used by the remote system when it responds to the PC's request in the Incoming Ports box.
5. Select the protocol used for **Incoming Ports** range from the pull-down list, either TCP, UDP, or All.
6. Select the **Enabled** option in the **Status** pull-down list.
7. Click the **Save** button to save the new rule.

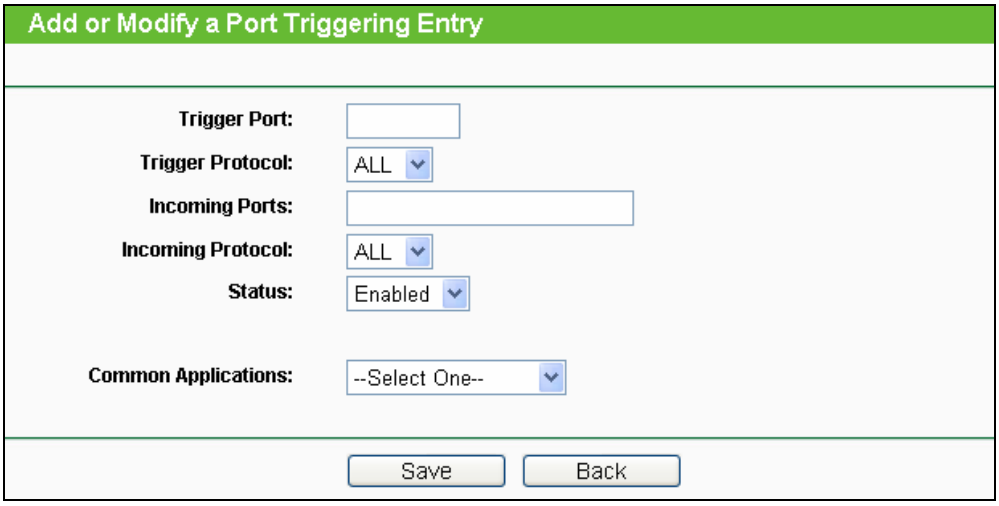


Figure 5-48 Add or Modify a Port Triggering Entry

There are many popular applications in the **Common Application** list. You can select an application and then the boxes of Trigger Port and Incoming Ports will be automatically filled in. This has the same effect as adding a new rule.

➢ **To modify or delete an existing entry**:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to enable all entries.

Click the **Disable All** button to disable all entries.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and Click the **Previous** button to return to the previous page.

☞ **Note:**

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **Incoming Ports** ranges cannot overlap each other.

5.9.3 DMZ

Choose menu "**Forwarding > DMZ**", and then you can view and configure DMZ host in the screen as shown in Figure 5-49.

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or video-conferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

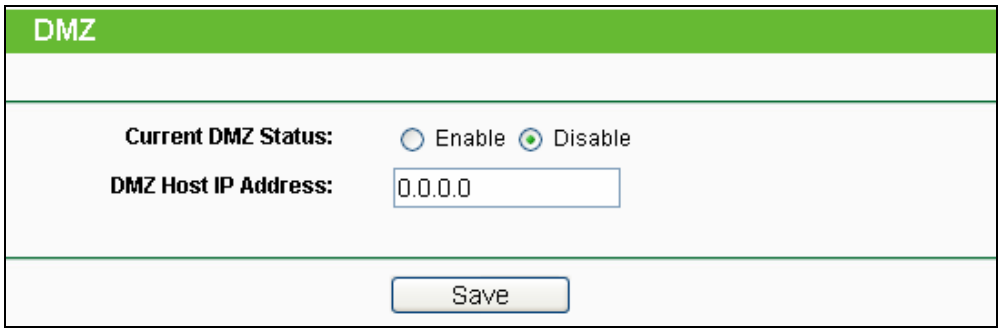


Figure 5-49 DMZ

➢ **To assign a computer or server to be a DMZ server**:

1. Click the **Enable** button.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

5.9.4 UPnP

Choose menu "**Forwarding > UPnP**", and then you can view the information about **UPnP** (Universal Plug and Play) in the screen as shown in Figure 5-50.

The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

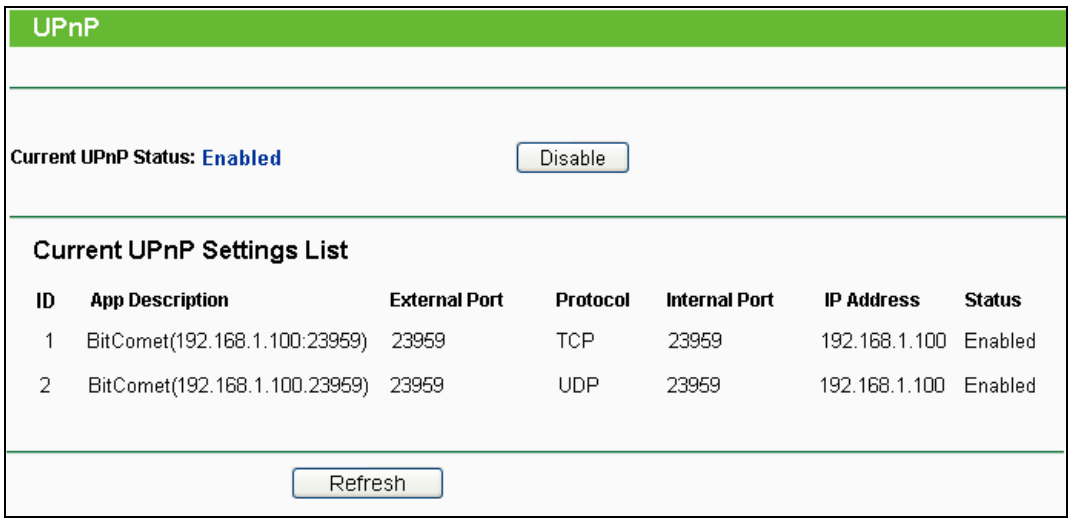


Figure 5-50 UPnP

- **Enable UPnP -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.
- **Current UPnP Settings List -** Displays the current UPnP information.
 - **App Description -** Description about the application which initiates the UPnP request.
 - **External Port -** Port that the Device opened for the application.
 - **Protocol -** Type of protocol that is opened.
 - **Internal Port -** Port that the Device opened for local host.
 - **IP Address -** IP address of the local host which initiates the UPnP request.
 - **Status -** Either Enabled or Disabled. "Enabled" means that port is still active; otherwise, the port is inactive.

Click the **Enable** button to enable UPnP.

Click the **Disable** button to disable UPnP.

Click the **Refresh** button to update the Current UPnP Settings List.

5.10 Security



Figure 5-51 The Security menu

There are four submenus under the Security menu as shown in Figure 5-51: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding function.

5.10.1 Basic Security

Choose menu "**Security > Basic Security**", and then you can configure the basic security in the screen as shown in Figure 5-52.

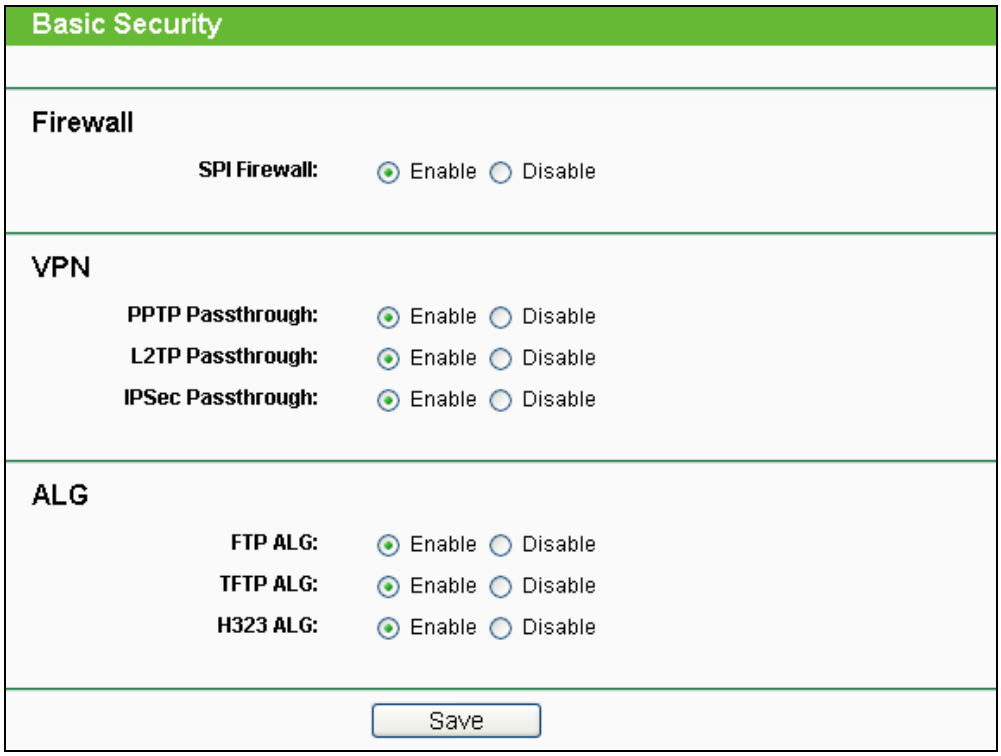


Figure 5-52 Basic Security

➢ **Firewall -** Here you can enable or disable the Device's firewall.

- **SPI Firewall** - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms

to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.

- **VPN -** VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Device.
 - **PPTP Passthrough -** PPTP (Point-to-Point Tunneling Protocol) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Device, click Enable.
 - **L2TP Passthrough -** L2TP (Layer Two Tunneling Protocol) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Device, click Enable.
 - **IPSec Passthrough -** IPSec (Internet Protocol security) is a suite of protocols for ensuring private, secure communications over IP (Internet Protocol) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Device, click **Enable**.
- **ALG -** It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
 - **FTP ALG -** To allow FTP clients and servers to transfer data across NAT, click Enable.
 - **TFTP ALG -** To allow TFTP clients and servers to transfer data across NAT, click Enable.
 - **H323 ALG -** To allow Microsoft NetMeeting clients to communicate across NAT, click Enable.

Click the **Save** button to save your settings.

5.10.2 Advanced Security

Choose menu “**Security > Advanced Security**”, and then you can protect the Device from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood in the screen as shown in Figure 5-53.

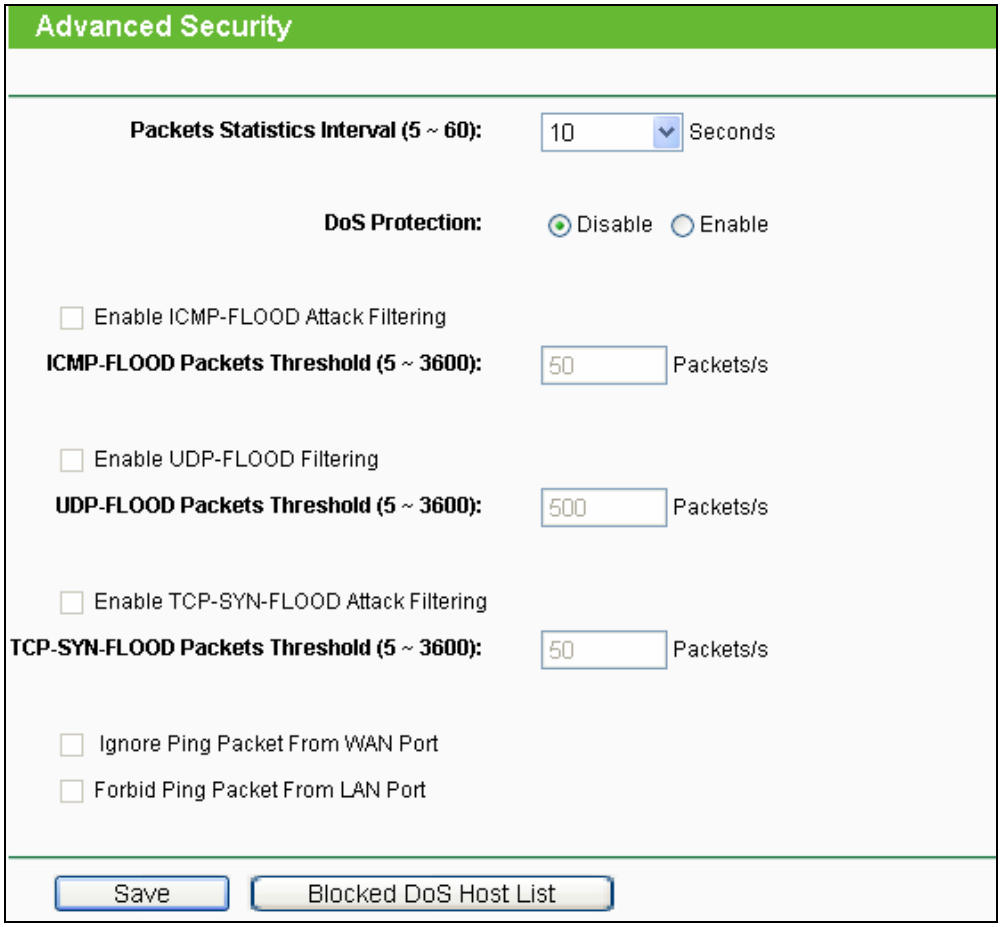


Figure 5-53 Advanced Security

Note:

FLOOD Filtering will take effect only when the **Traffic Statistics** in **System Tools** is enabled.

- **Packets Statistics interval (5~60) -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by ICMP-Flood, UDP Flood and TCP-SYN Flood.
- **DoS Protection -** Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
- **Enable ICMP-FLOOD Attack Filtering -** Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600) -** The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Device will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering -** Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600) -** The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Device will start up the blocking function immediately.

- **Enable TCP-SYN-FLOOD Attack Filtering -** Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- **TCP-SYN-FLOOD Packets Threshold (5~3600) -** The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Device will start up the blocking function immediately.
- **Ignore Ping Packet From WAN Port -** Enable or Disable Ignore Ping Packet From WAN Port. The default setting is Disabled. If enabled, the ping packet from Internet cannot access the Device.
- **Forbid Ping Packet From LAN Port -** Enable or Disable Forbid Ping Packet From LAN Port. The default setting is Disabled. If enabled, the ping packet from LAN cannot access the Device and defend against some viruses.

Click the **Save** button to save the settings.

Click the **Blocked DoS Host List** button to display the DoS host table by blocking.

5.10.3 Local Management

Choose menu "**Security > Local Management**", and then you can configure the management rule in the screen as shown in Figure 5-54. The management feature allows you to deny computers in LAN from accessing the Device.

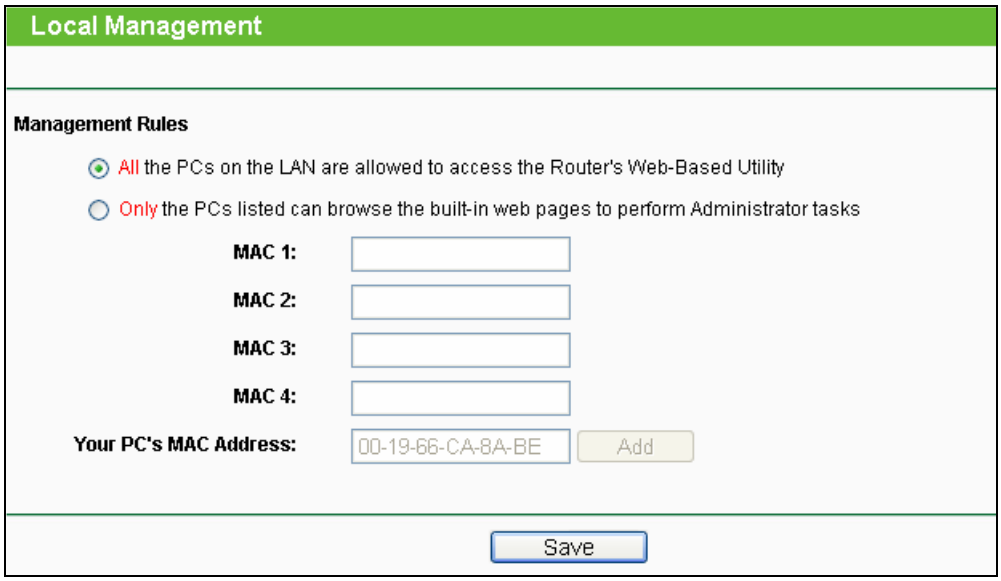


Figure 5-54 Local Management

By default, the radio button **All the PCs on the LAN are allowed to access the Router's Web-Based Utility** is selected. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Device's Web-Based Utility locally, from inside the network, click the radio button **Only the PCs listed can browse the built-in web pages to perform Administrator tasks**, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with the MAC address listed can

use the password to browse the built-in web pages to perform Administrator tasks and all the others will be blocked.

After click the **Add** button, your PC's MAC Address will be placed in the Control List above.

Click the **Save** button to save your settings.

☞ **Note:**

If your PC is blocked and you want to access the Device again, use a pin to press and hold the **Reset Button** on the back panel about 5 seconds to reset the Device's factory defaults in the Device's Web-Based Utility.

5.10.4 Remote Management

Choose menu "**Security > Remote Management**", and then you can configure the Remote Management function in the screen as shown in Figure 5-55. This feature allows you to manage your Device from a remote location via the Internet.

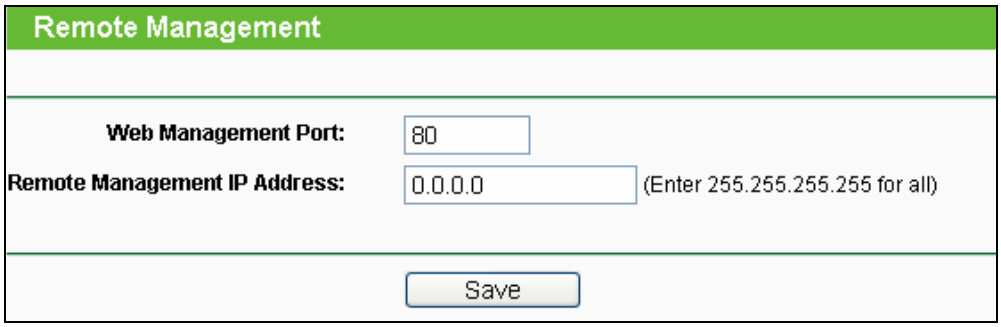


Figure 5-55 Remote Management

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This Device's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65535 but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your Device from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function you should change 0.0.0.0 to a valid IP address. If set to be 255.255.255.255, then all the hosts can access the Device from Internet.

To access the Device, you should enter your Device's WAN IP address into your browser's address (in IE) or location (in Netscape) box, followed by a colon and the custom port number you set in the Web Management Port box.

- For example, if your Device's WAN address is 202.96.12.8 and you use port number 8080, enter http://202.96.12.8:8080 in your browser. You will be asked for the Device's password.

After successfully entering the password, you will be able to access the Device's web-based utility.

☞ **Note:**

Be sure to change the Device's default password to a secure password.

5.11 Parental Control

Choose menu "**Parental Control**", and then you can configure the parental control in the screen as shown in Figure 5-56. The Parental Control function can be used to control the Internet activities of the children, their access to certain websites, as well as the time of surfing.

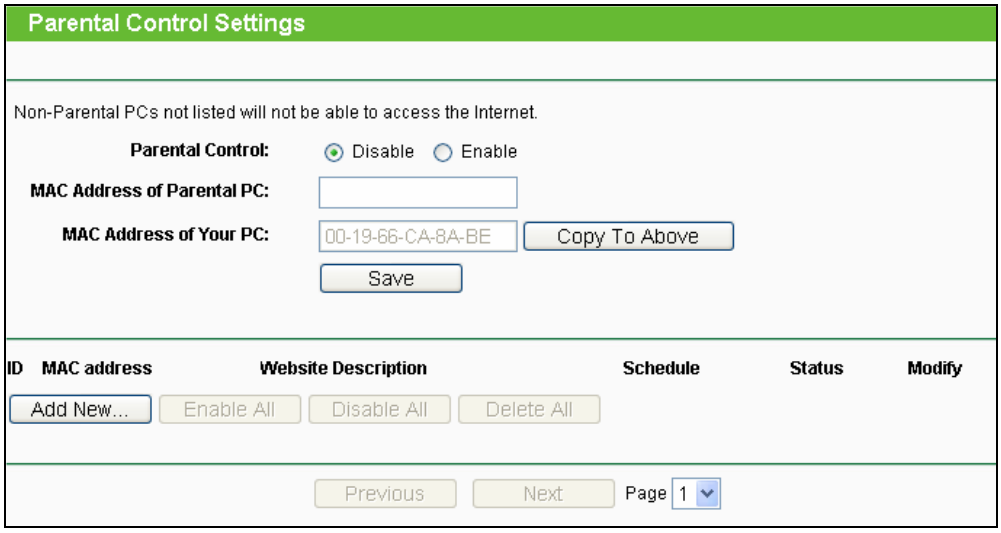


Figure 5-56 Parental Control Settings

- **Parental Control -** Check **Enable** if you want this function to take effect; otherwise check **Disable**.
- **MAC Address of Parental PC -** In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.
- **MAC Address of Your PC -** This field displays the MAC address of the PC that is managing this Device. If the MAC Address of your adapter is registered, you can click the **Copy To Above** button to fill this address to the MAC Address of Parental PC field above.
- **Website Description -** Description of the allowed website for the PC controlled.
- **Schedule -** The time period allowed for the PC controlled to access the Internet. For detailed information, please go to **Access Control > Schedule**.
- **Modify -** Here you can edit or delete an existing entry.

➢ **For example**: If you desire that the children's PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below:

1. Click **Parental Control** menu on the left to enter the Parental Control Settings page. Check **Enable** and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.
2. Click **Access Control > Schedule** on the left to enter the **Schedule** Settings page. Click **Add New...** button to create a new schedule with Schedule Description is **Schedule_1**, Day is **Sat** and Time is **"all day-24 hours"**.
3. Click **Parental Control** menu on the left to go back to the Parental Control Settings page, and then follow the instructions below.

1) Click **Add New...** button.

2) Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.

3) Enter **Allow Google** in the **Website Description** field.

4) Enter **www.google.com** in the **Allowed Domain Name** field.

5) Select **Schedule_1** you create just now from the **Effective Time** drop-down list.

6) In **Status** field, select **Enable**.

7) Click **Save** to complete the settings.

4. Then you will go back to the **Parental Control** Settings page and see the following list.

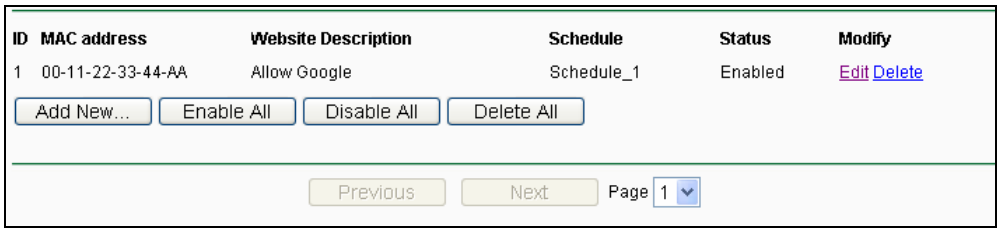


Figure 5-57 Parental Control List

Click the **Add New...** button to add a new Parental Control entry.

Click the **Enable All** button to enable all the rules in the list.

Click the **Disable All** button to disable all the rules in the list.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

5.12 Access Control



Figure 5-58 Access Control

There are four submenus under the Access Control menu as shown in Figure 5-58: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

The Device, providing convenient and strong **Internet access control** function, can control the Internet activities of hosts in the LAN. Moreover, you can flexibly combine the **Host List**, **Target List** and **Schedule** to restrict the Internet surfing of these hosts.

5.12.1 Rule

Choose menu "**Access Control > Rule**", and then you can view and set Access Control rules in the screen as shown in Figure 5-59.

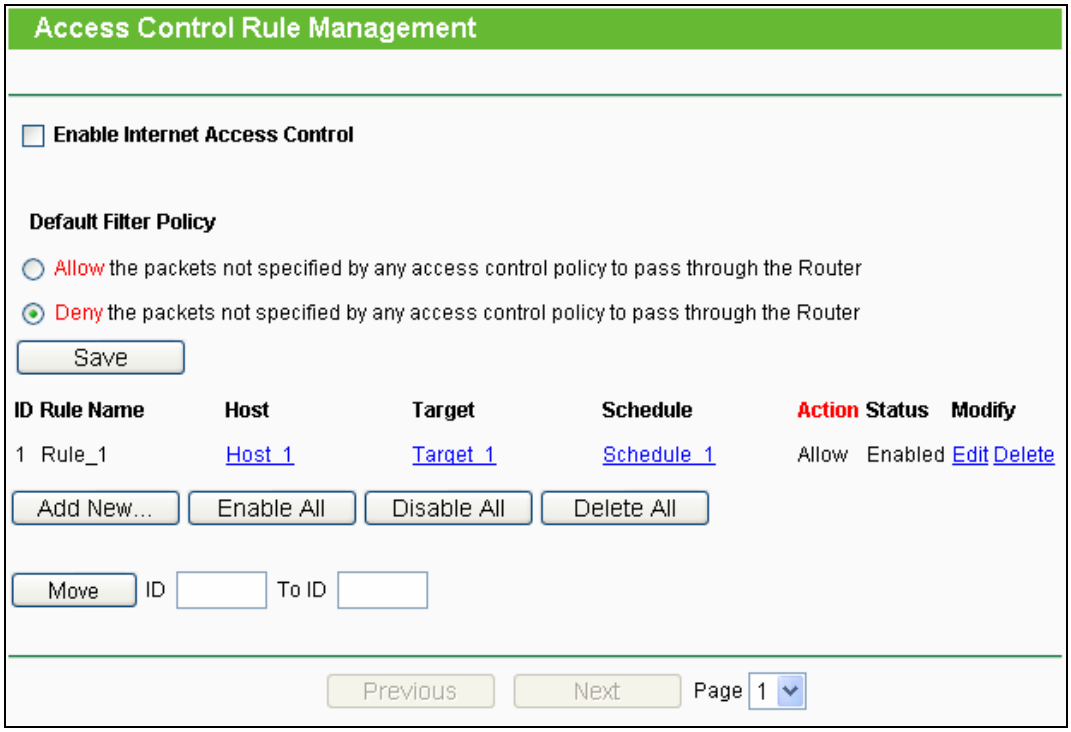


Figure 5-59 Access Control Rule Management

- **Enable Internet Access Control -** Select the check box to enable the Internet Access Control function, and then the **Default Filter Policy** can take effect.
- **Rule Name -** Here displays the name of the rule and this name is unique.
- **Host -** Here displays the host selected in the corresponding rule.
- **Target -** Here displays the target selected in the corresponding rule.
- **Schedule -** Here displays the schedule selected in the corresponding rule.
- **Action -** Here displays the action the Device takes to deal with the packets. It could be **Allow** or **Deny**. **Allow** means that the Device permits the packets to go through the Device. **Deny** means that the Device rejects the packets to go through the Device.
- **Status -** This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
- **Modify -** Here you can edit or delete an existing rule.

- **For example**: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click the submenu **Host** of **Access Control** on the left to enter the **Host Setting** page. Add a new entry with the Host Description as Host_1 and MAC Address as 00-11-22-33-44-AA.
2. Click the submenu **Target** of **Access Control** on the left to enter the **Target Settings** page. Add a new entry with the Target Description as Target_1 and Domain Name as www.google.com.
3. Click the submenu **Schedule** of **Access Control** on the left to enter the **Schedule Settings** page. Add a new entry with the Schedule Description as Schedule_1, Day as Sat and Sun, Start Time as 1800 and Stop Time as 2000.
4. Click the submenu **Rule** of **Access Control** on the left to return to the **Rule Management** page. Select **Enable Internet Access Control** and choose "**Deny the packets not specified by any Internet access control rule to pass through the Router**".
5. Click **Add New...** button to add a new rule as follows:

1) In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
2) In Host field, select Host_1.
3) In Target field, select Target_1.

4) In Schedule field, select Schedule_1.

5) In Action field, select Allow.

6) In Status field, select Enable.

7) Click **Save** to complete the settings.

6. Then you will go back to the **Access Control Rule Management** page and see the following list.

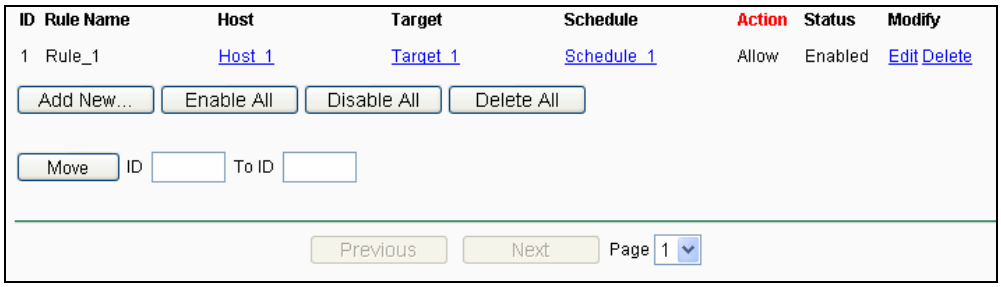


Figure 5-60 Access Control List

Click the **Add New...** button to add a new host list entry.

Click the **Enable All** button to enable all the rules in the list.

Click the **Disable All** button to disable all the rules in the list.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

5.12.2 Host

Choose menu "**Access Control > Host**", and then you can view and set a Host list in the screen as shown in Figure 5-61. The host list is necessary for the Access Control Rule.

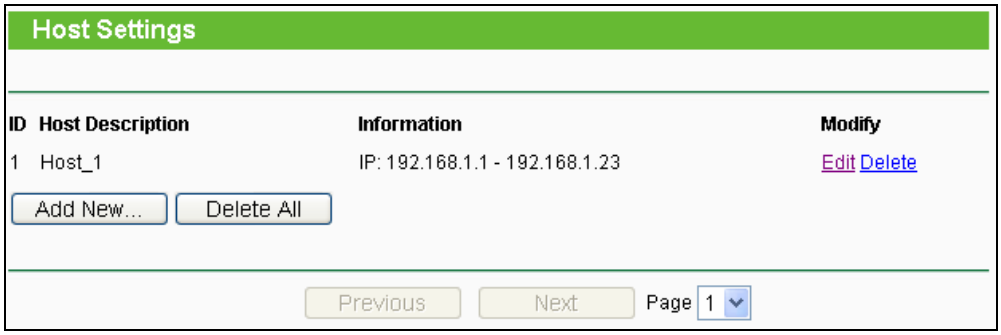


Figure 5-61 Host Settings

- **Host Description** - Here displays the description of the host and this description is **unique**.
- **Information** - Here displays the information about the host. It can be IP or MAC.

- **Modify** - To modify or delete an existing entry.

- **For example**: If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA, you should follow the settings below:

1. Click **Add New...** button to enter the **Add or Modify a Host Entry** page.
2. In Mode field, select MAC Address from the drop-down list.
3. In Host Name field, create a unique description for the host, for example Host_1.
4. In MAC Address field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete the settings.
6. Go back to the **Host Settings** page and you will see the following list.

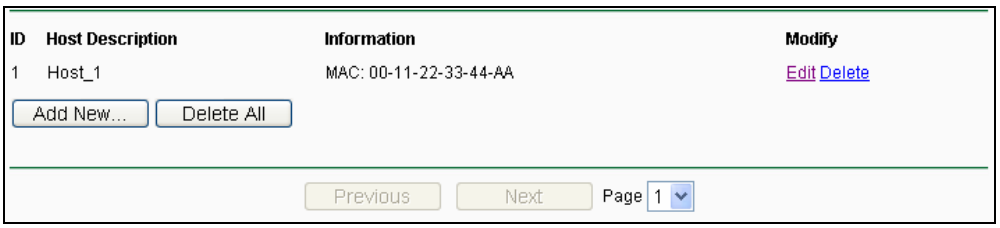


Figure 5-62 Host List

Click the **Add New...** button to add a new host list entry.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

5.12.3 Target

Choose menu "**Access Control > Target**", and then you can view and set a Target list in the screen as shown in Figure 5-63. The target list is necessary for the Access Control Rule.

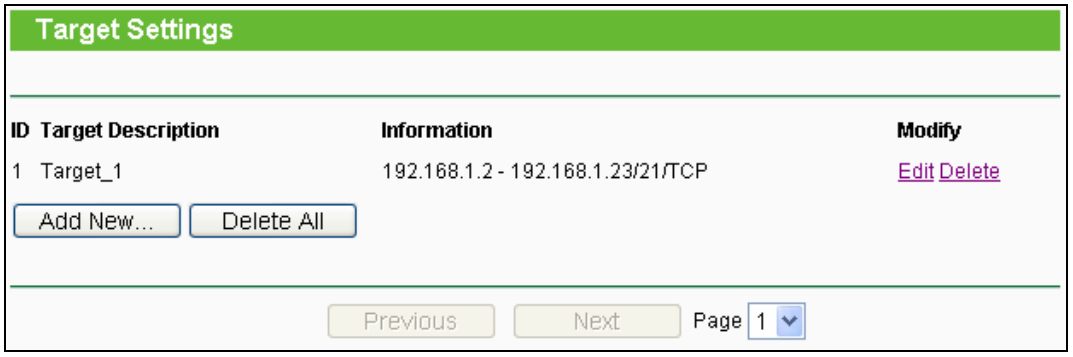


Figure 5-63 Target Settings

- **Target Description** - Here displays the description about the target and this description is **unique**.
- **Information** - The target can be IP address, port, or domain name.
- **Modify** - To modify or delete an existing entry.
- **For example**: If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access www.google.com only, you should first follow the settings below:

1. Click **Add New…** button to enter **Add or Modify an Access Target Entry** page.
2. In Mode field, select Domain Name from the drop-down list.
3. In Target Description field, create a unique description for the target, for example Target_1.
4. In Domain Name field, enter www.google.com.
5. Click **Save** to complete the settings.
6. Go back to the **Target Settings** page and see the following list

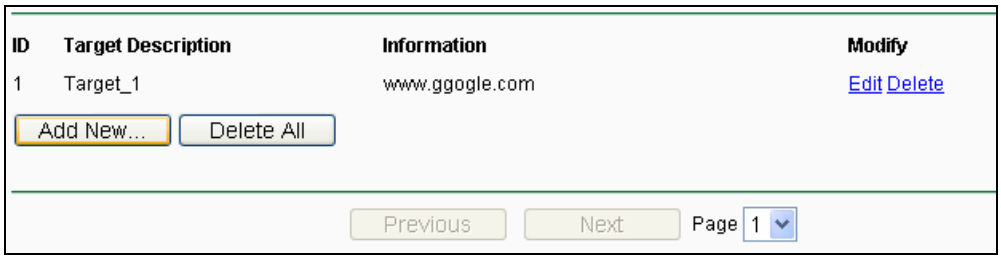


Figure 5-64 Access Target List

Click the **Add New...** button to add a new target entry.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

5.12.4 Schedule

Choose menu "**Access Control > Schedule**", you can view and set a Schedule list in the next screen as shown in Figure 5-65. The Schedule list is necessary for the Access Control Rule.

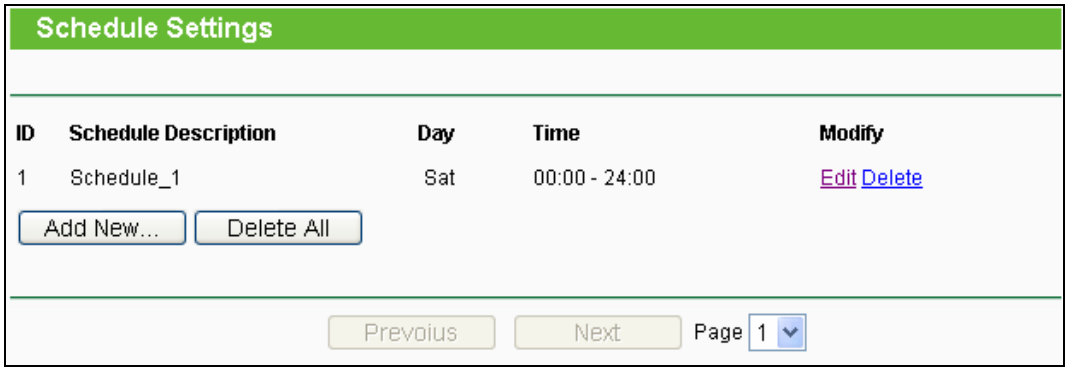


Figure 5-65 Schedule Settings

- **Schedule Description** - Here displays the description of the schedule and this description is **unique**.
- **Day** - Here displays the day(s) in a week.
- **Time** - Here displays the time period in a day.
- **Modify** - Here you can edit or delete an existing schedule.
- **For example**: If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, you should first follow the settings below:

1. Click **Add New...** button to enter the **Advance Schedule Settings** page.
2. In Schedule Description field, create a unique description for the schedule, for example Schedule_1.
3. In Day field, choose **Select Days** and select Sat and Sun.
4. In Time field, enter 1800 in Start Time and 2000 in Stop Time.
5. Click **Save** to complete the settings.
6. Go back to the **Schedule Settings** page and see the following list

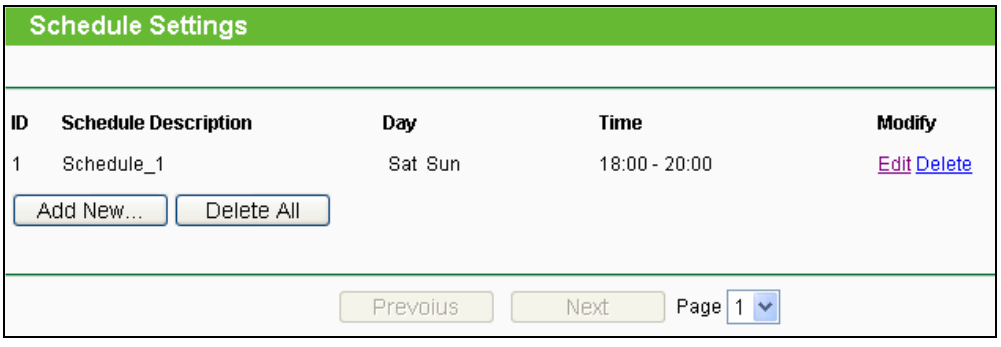


Figure 5-66 Schedule List

Click the **Add New...** button to add a new target entry.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

5.13 Static Routing



Figure 5-67 Static Routing

There is only one submenu under the Static Routing menu as shown in Figure 5-67: **Static Routing List**. Click it, and you will be able to configure the corresponding function.

Choose menu "**Static Routing > Static Routing List**", and then you can configure the static route in the next screen (shown in Figure 5-68).

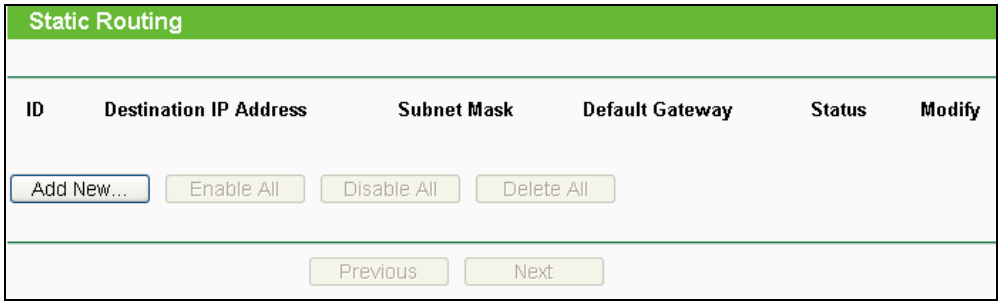


Figure 5-68

A static route is a pre-determined path that network information must follow to reach a specific host or network. Use the **Static Routing** page to add or delete a route.

➢ **To add static routing entries**:

1. Click the **Add New...** button.
2. Enter the following data:

Destination IP Address - The address of the network or host that you want to assign to a static route

Subnet Mask - Determines which portion of an IP address is the network portion, and which portion is the host portion.

Default Gateway - The IP address of the default gateway device that allows for the contact between the Device and the network or host

3. Select the **Enabled** in the **Status** pull-down list.

4. Click the **Save** button to save the changes.

➢ **To modify or delete an existing entry**:

1. Find the desired entry in the table.

2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to enable all entries.

Click the **Disable All** button to disable all entries.

Click the **Delete All** button to delete all entries.

5.14 Bandwidth Control



Figure 5-69 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 5-69: **Control Settings** and **Rules List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.14.1 Control Settings

Choose menu "**Bandwidth Control > Control Settings**", and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen (shown in Figure 5-70). Their values should be configured less than 1000000Kbps.

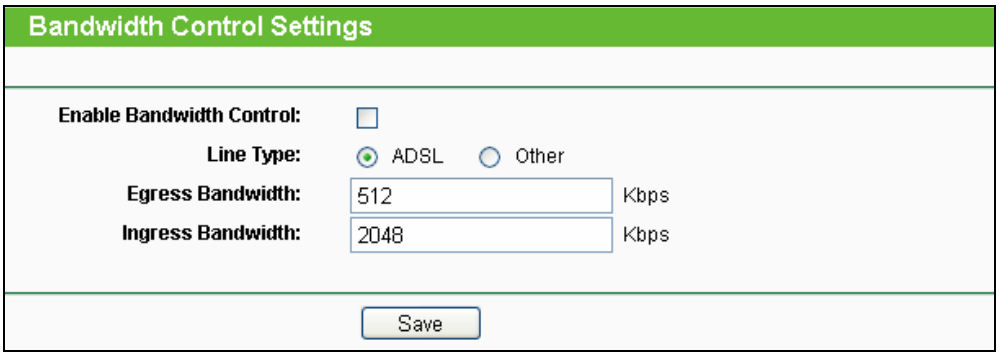


Figure 5-70 Bandwidth Control Settings

- **Enable Bandwidth Control -** If enabled, the Bandwidth Control rules will take effect.
- **Egress Bandwidth -** The upload speed through the WAN port.
- **Ingress Bandwidth -** The download speed through the WAN port.

5.14.2 Rules List

Choose menu "**Bandwidth Control > Rules List**", and then you can view and configure the Bandwidth Control rules in the screen below.

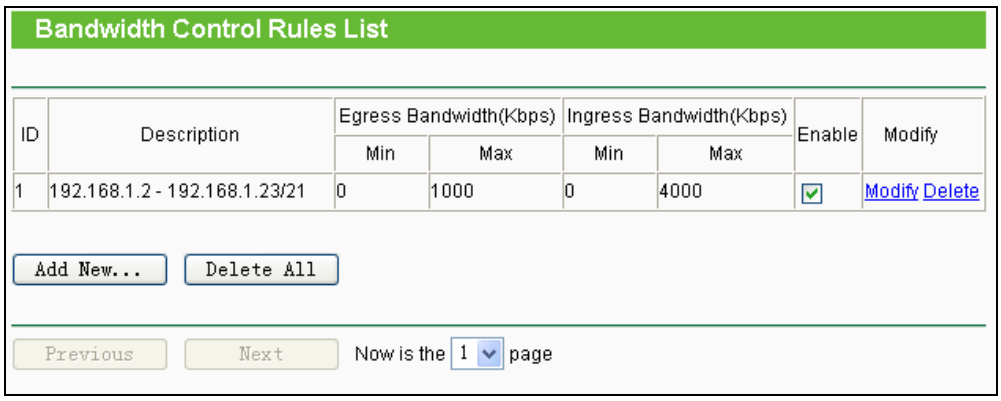


Figure 5-71 Bandwidth Control Rules List

- **ID -** The sequence of entry.
- **Description -** The information of description include address range, the port range and protocol of transport layer.
- **Egress Bandwidth -** The max upload speed which through the WAN port. The default number is 0.
- **Ingress Bandwidth -** The max download speed which through the WAN port. The default number is 0.
- **Enable -** Rule status, which shows whether the rule takes effect.
- **Modify -** Choose to modify or delete an existing entry.

5.15 IP& MAC Binding

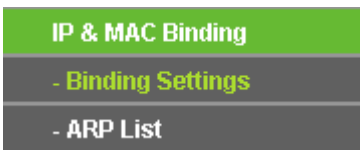


Figure 5-72 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 5-72): **Binding Settings** and **ARP List**. Click either of them, and you will be able to view or configure the corresponding function. The detailed explanations for each submenu are provided below.

5.15.1 Binding Settings

Choose menu "**IP&MAC Binding > Binding Settings**", and then you can view and configure the IP&MAC Binding in the screen below.

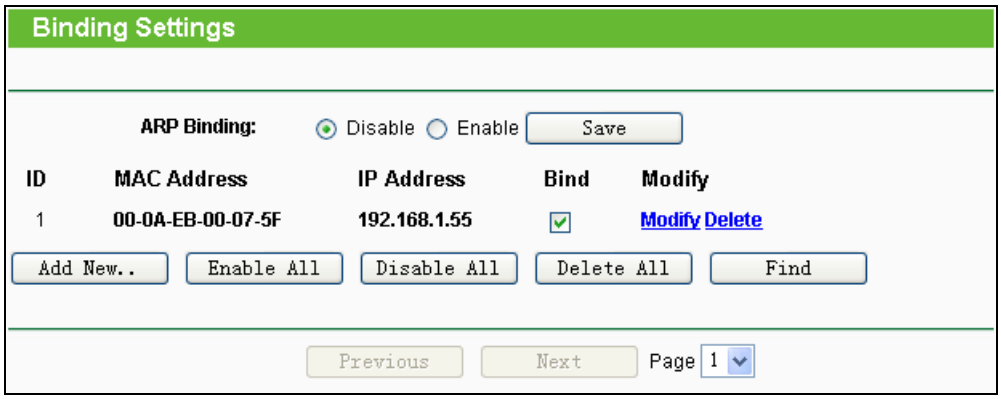


Figure 5-73 Binding Settings

- **MAC Address -** The MAC address of the controlled computer in the LAN.
- **IP Address -** The assigned IP address of the controlled computer in the LAN.
- **Bind -** Check this option to enable ARP binding for a specific device.
- **Modify -**To modify or delete an existing entry.

- **Add New… -** Click the **Add New…** button to add a new entry to the table.
- **Enable All -** Click the **Enable All** button to enable all entries.
- **Disable All -** Click the **Disable All** button to disable all entries.
- **Delete All -** Click the **Delete All** button to delete all entries.
- **Find -** To find existed entry you want.

5.15.2 ARP List

Choose menu "**IP&MAC Binding > ARP List**", and then you can view and configure the ARP List in the screen below shown in Figure 5-74.

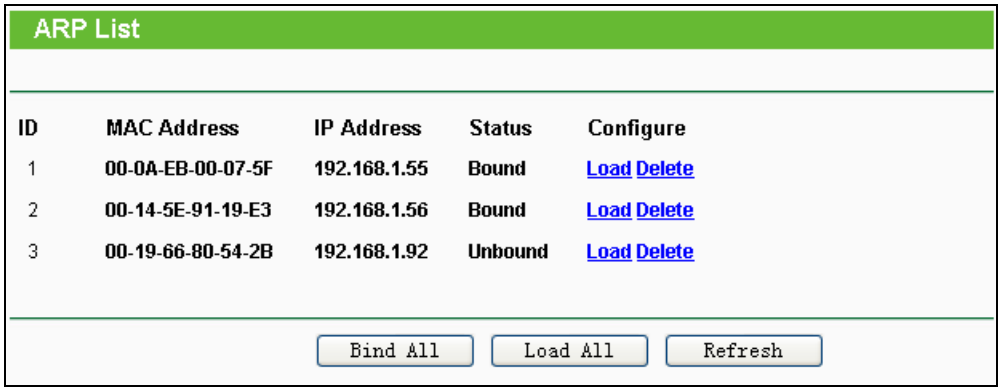


Figure 5-74 ARP List

- **MAC Address -** The MAC address of a controlled computer in the LAN.
- **IP Address -** The assigned IP address of a controlled computer in the LAN.
- **Status -** Indicates whether or not the MAC and IP addresses are bound.
- **Configure -** These buttons are for loading or deleting an item.
 - **Load -** Load the item to the IP & MAC Binding list.
 - **Delete -** Delete the item from the list.
- **Bind All -** Bind all current items. This option is only available when ARP Binding is enabled and saved in the Binding Setting page.
- **Load All -** Load all items into the IP & MAC Binding list.

☞ **Note:**

An item can not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items have no interference with the IP & MAC Binding list.

5.16 Dynamic DNS

The Device offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Device. Before using this feature, you

need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

1. If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 5-75.

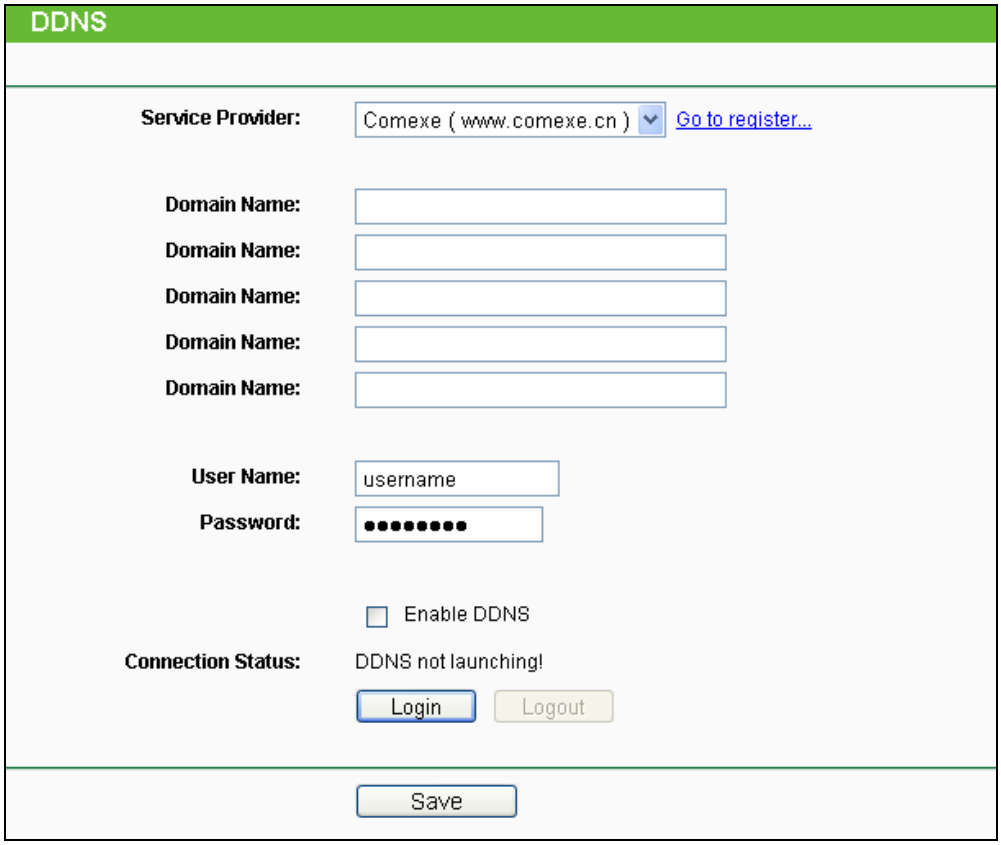


Figure 5-75 Comexe.cn DDNS Settings

➢ **To set up for DDNS, follow these instructions:**

1) Enter the **Domain Names** your dynamic DNS service provider gave.

2) Enter the **User Name** for your DDNS account.

3) Enter the **Password** for your DDNS account.

4) Click the **Login** button to login the DDNS service.

➢ **Connection Status** - The status of the DDNS service connection is displayed here.

Click **Logout** to logout the DDNS service.

☞ **Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

2. If the dynamic DNS **Service Provider** you select is www.dyndns.org, the page will appear as shown in Figure 5-76.

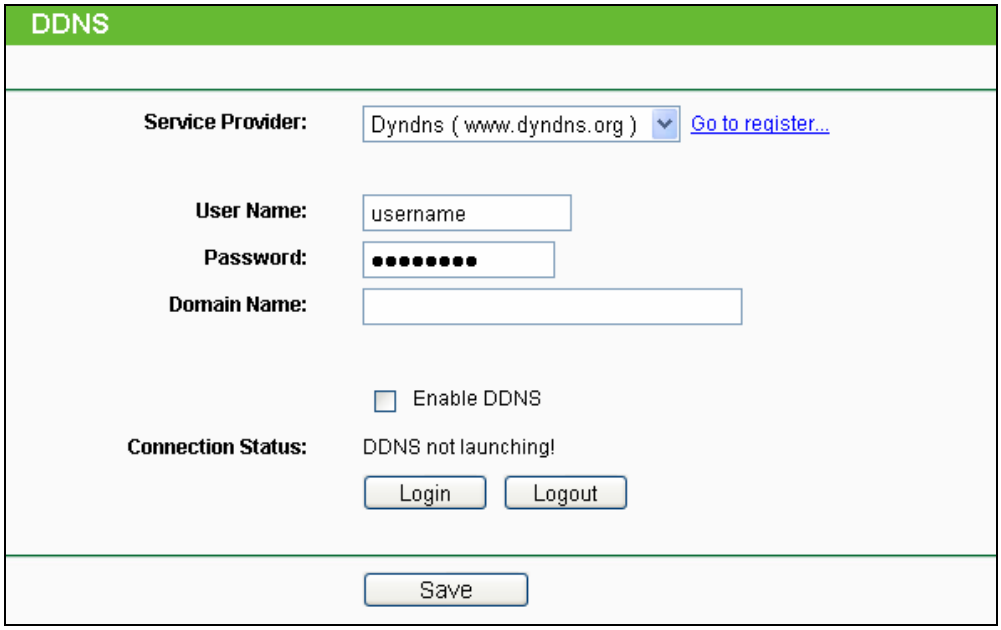


Figure 5-76 Dyndns.org DDNS Settings

➢ **To set up for DDNS, follow these instructions:**

1) Enter the User Name for your DDNS account.
2) Enter the Password for your DDNS account.
3) Enter the Domain Name you received from dynamic DNS service provider.
4) Click the Login button to login to the DDNS service.

➢ **Connection Status** - The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

☞ **Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

3. If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in Figure 5-77.

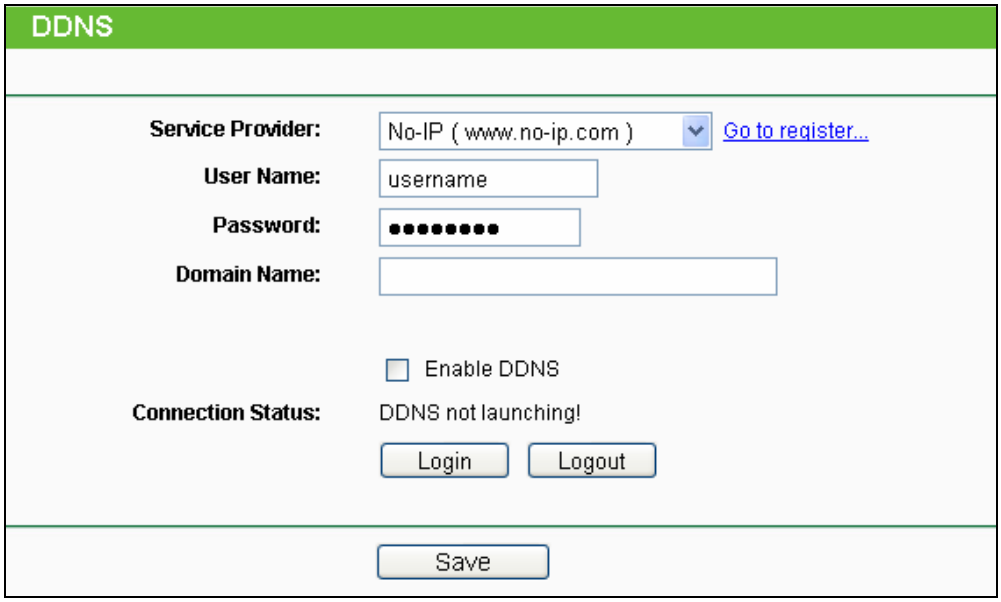


Figure 5-77 No-ip.com DDNS Settings

➢ **To set up for DDNS, follow these instructions:**

1. Enter the User Name for your DDNS account.
2. Enter the Password for your DDNS account.
3. Enter the Domain Name you received from dynamic DNS service provider.
4. Click the Login button to login to the DDNS service.

➢ **Connection Status** - The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

☞ **Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

5.17 System Tools



Figure 5-78 The System Tools menu

There are nine submenus under the **System Tools** main menu (as shown in Figure 5-78): **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults, Backup & Restore, Reboot, Password, System Log** and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.17.1 Time Settings

Choose menu "**System Tools > Time Settings**", and then you can configure the time on the following screen.

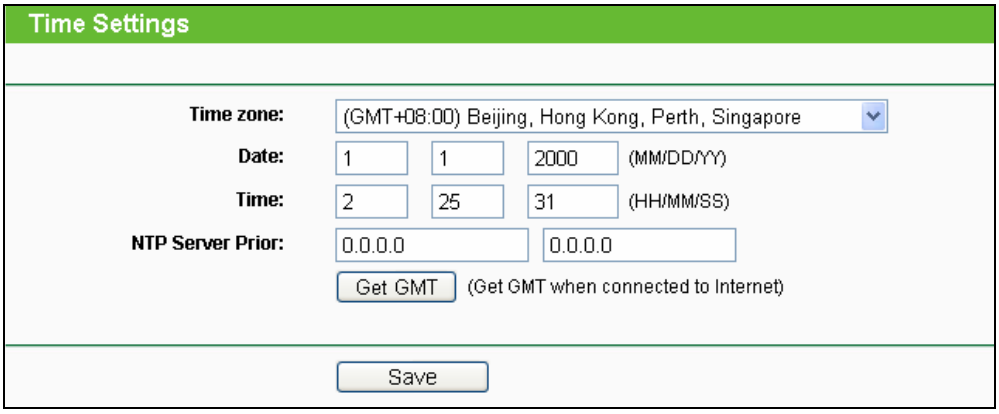


Figure 5-79 Time settings

- **Time Zone -** Select your local time zone from this pull down list.

- **To set time manually:**

1. Select your local time zone.
2. Enter the **Date** in Month/Day/Year format.

3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

➢ **For automatic time synchronization:**

1. Enter the address of the **NTP Server Prior**.
2. Click the **Get GMT** button to get GMT from the Internet.

☞ **Note:**

1. This setting will be used for some time-based functions such as firewall functions. These time-dependant functions will not work if time is not set. So, it is important to specify time settings as soon as you successfully login to the Device.
2. The time will be lost if the Device is turned off.
3. The Device will automatically obtain GMT from the Internet if it is configured accordingly.

5.17.2 Diagnostic

Choose menu "**System Tools > Diagnostic**", and then you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

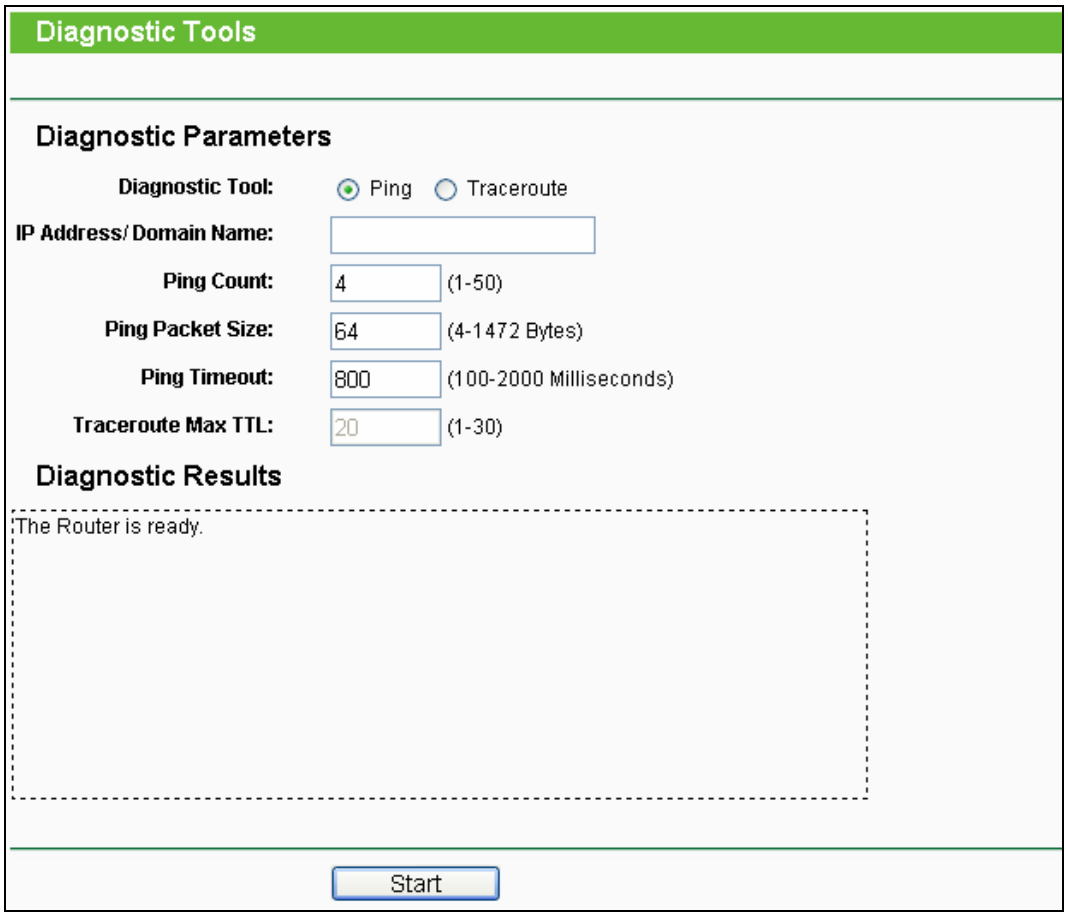


Figure 5-80 Diagnostic Tools

- **Diagnostic Tool -** Click the radio button to select one diagnostic tool:
 - **Ping -** This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
 - **Traceroute -** This diagnostic tool tests the performance of a connection.

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/ Domain Name** - Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
- **Ping Count** - Specifies the number of Echo Request messages sent. The default is 4.
- **Ping Packet Size** - Specifies the number of data bytes to be sent. The default is 64.
- **Ping Timeout** - Time to wait for a response, in milliseconds. The default is 800.

➢ **Traceroute Max TTL** - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click the **Start** button to start the diagnostic procedure.

The **Diagnostic Results** page (as shown in Figure 5-81) displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

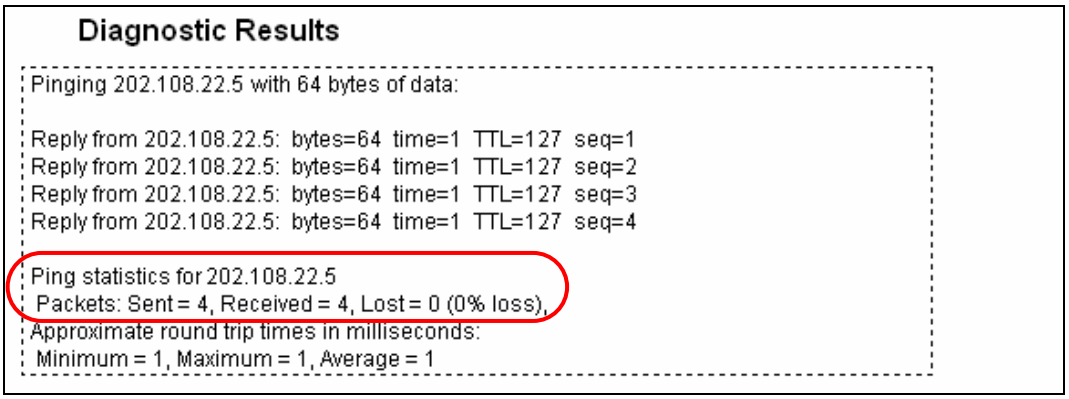


Figure 5-81 Diagnostic Results

☞ **Note:**

1. Only one user can use the diagnostic tools at one time.
2. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters, and "Traceroute Max TTL" is Traceroute Parameter.

5.17.3 Firmware Upgrade

Choose menu "**System Tools > Firmware Upgrade**", and then you can update the latest version of firmware for the Device on the following screen.

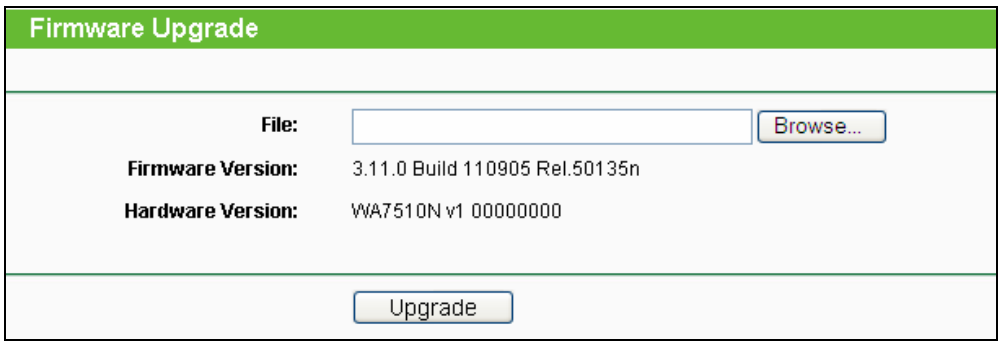


Figure 5-82 Firmware Upgrade

➢ **To upgrade the Device's firmware, follow these instructions:**

1. Download a most recent firmware upgrade file from our website (www.tp-link.com).

2. Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
3. Click the **Upgrade** button.
4. The Device will reboot while the upgrading has been finished.

- **Firmware Version** - Displays the current firmware version.
- **Hardware Version** - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note:

The firmware version must correspond to the hardware. The upgrade process takes a few moments and the Device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the Device.

5.17.4 Factory Defaults

Choose menu "**System Tools > Factory Defaults**", and you can restore the configurations of the Device to factory defaults on the following screen.

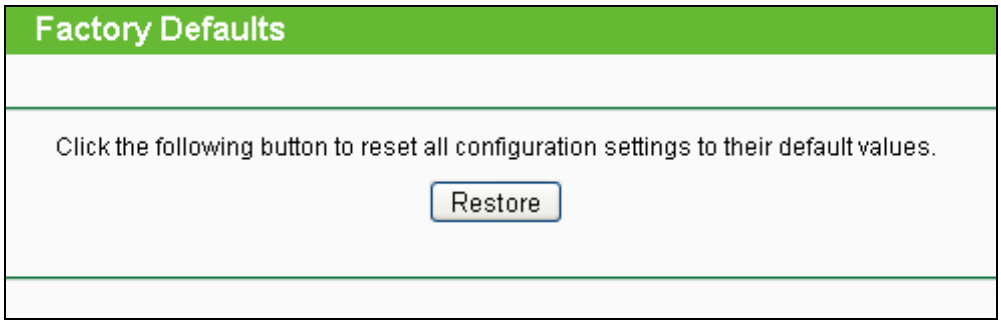


Figure 5-83 Restore Factory Default

Click the **Restore** button to reset all configuration settings to their default values.

- Default User Name **- admin**.
- Default Password **- admin**.
- Default IP Address **- 192.168.1.254**.
- Default Subnet Mask **- 255.255.255.0**.

Note:

All changed settings will be lost when defaults are restored.

5.17.5 Backup & Restore

Choose menu "**System Tools > Backup & Restore**", and then you can save the current configuration of the Device as a backup file and restore the configuration via a backup file as shown in Figure 5-84.



Figure 5-84 Backup & Restore

Click the **Backup** button to save all configuration settings to your local computer as a file.

➢ To restore the AP's configuration, follow these instructions:

1. Click the **Browse** button to find the configuration file which you want to restore.
2. Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

☞ **Note:**

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the AP will restart automatically then. Keep the power of the AP on during the process, in case of any damage.

5.17.6 Reboot

Choose menu "**System Tools > Reboot**", and then you can click the **Reboot** button to reboot the Device via the next screen.



Figure 5-85 Reboot the Device

Click the **Reboot** button to reboot the Device.

➢ Some settings of the Device will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Device (system will reboot automatically.).
- Restore the Device's settings to the factory defaults (system will reboot automatically.).
- Update the configuration with the file (system will reboot automatically.).

5.17.7 Password

Choose menu "**System Tools > Password**", and then you can change the factory default user name and password of the Device in the next screen as shown in Figure 5-86.

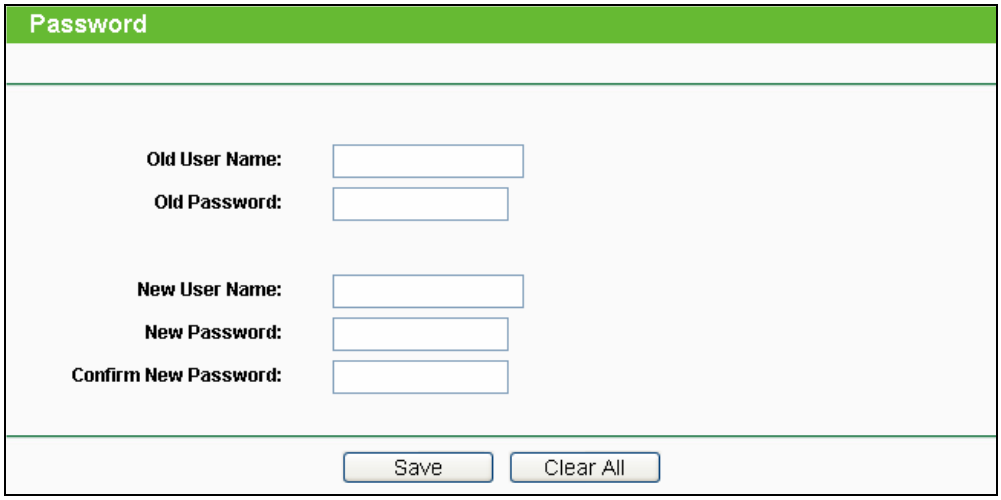


Figure 5-86 Password

It is strongly recommended that you change the factory default user name and password of the AP. All users who try to access the AP's web-based utility will be prompted for the AP's user name and password.

☞ **Note:**

The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

5.17.8 System log

Choose menu "**System Tools > System Log**", and then you can view the logs of the Device.

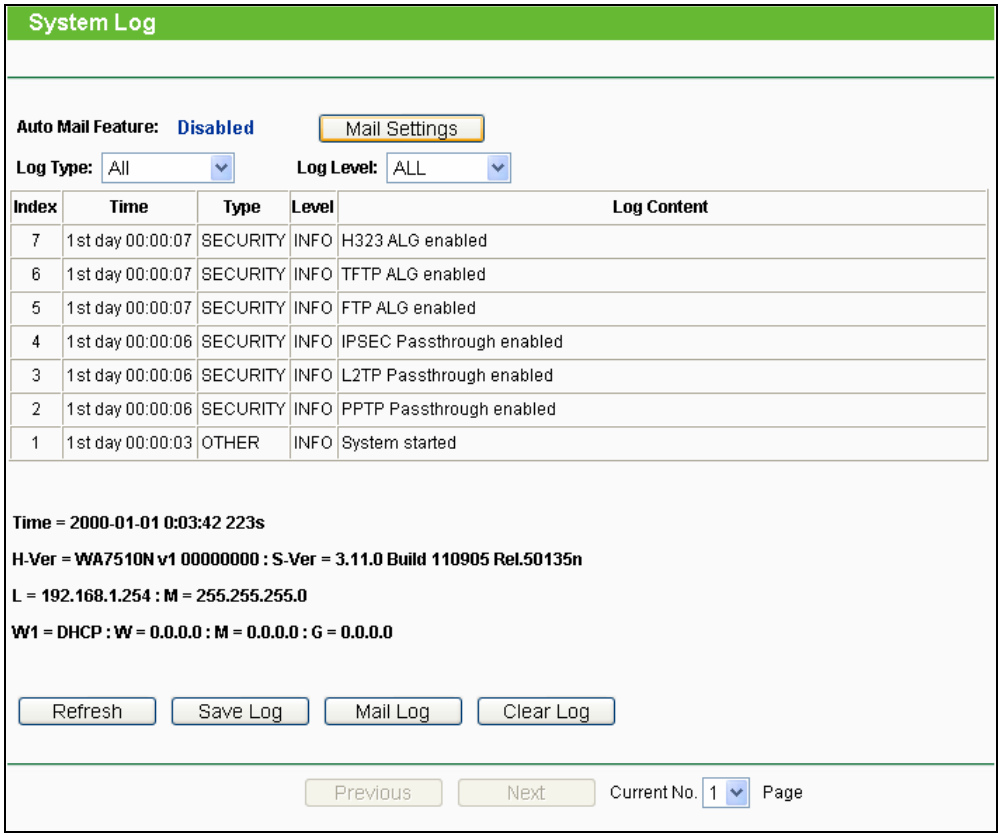


Figure 5-87 System Log

- **Auto Mail Feature -** Indicates whether auto mail feature is enabled or not.
- **Mail Settings -** Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

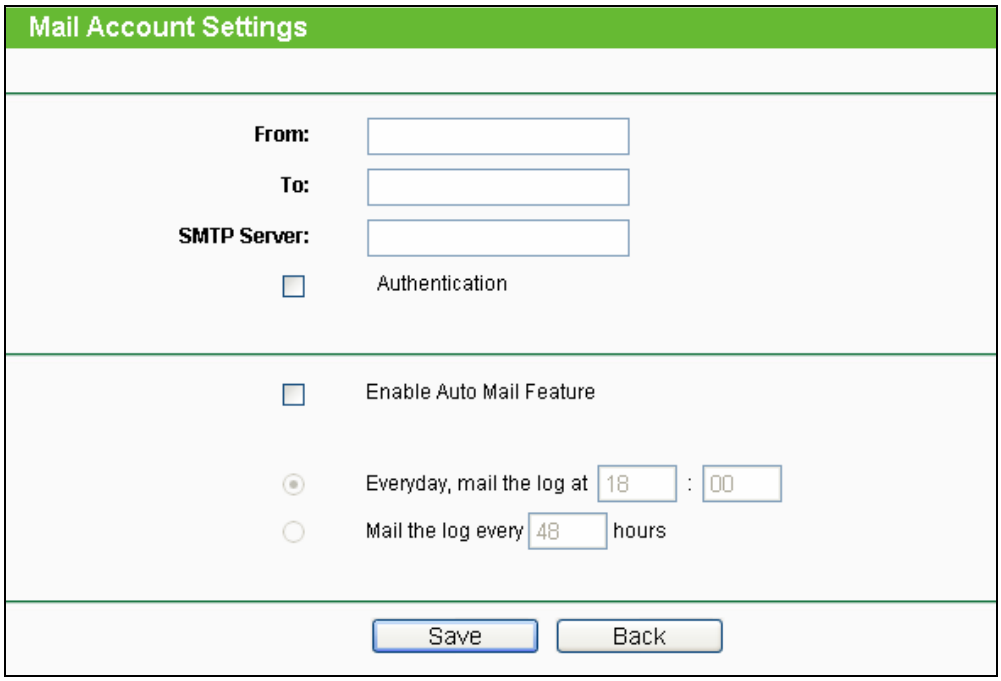


Figure 5-88 Mail Account Settings

- **From -** Your mail box address.
- **To -** Recipient's address.
- **SMTP Server -** Your SMTP server.
- **Authentication -** Most SMTP Server requires Authentication.

Note:

Only when you select **Authentication**, do you have to enter the User Name and Password in the following fields.

- **User Name -** Your mail account name.
- **Password -** Your mail account password.
- **Auto Mail Feature** will help you monitor how your Device is running.

Everyday, at specified time, the Device will automatically send the log to specified mailbox.

Every few hours, such as 2 hours, the Device will automatically send the log to specified mailbox.

- **Log Type -** By selecting the log type, only logs of this type will be shown.
- **Log Level -** By selecting the log level, only logs of this level will be shown.
- **Refresh -** Refresh the page to show the latest log list.

- **Save Log -** Click to save all the logs in a txt file.
- **Mail Log -** Click to send an email of current logs manually according to the address and validation information set in Mail Settings. The result will be shown in the later log soon.
- **Clear Log -** All the logs will be deleted from the Device permanently, not just from the page.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

5.17.9 Statistics

Choose menu "**System Tools > Statistics**", and then you can view the statistics of the Device, including total traffic and current traffic of the last Packets Statistic Interval.

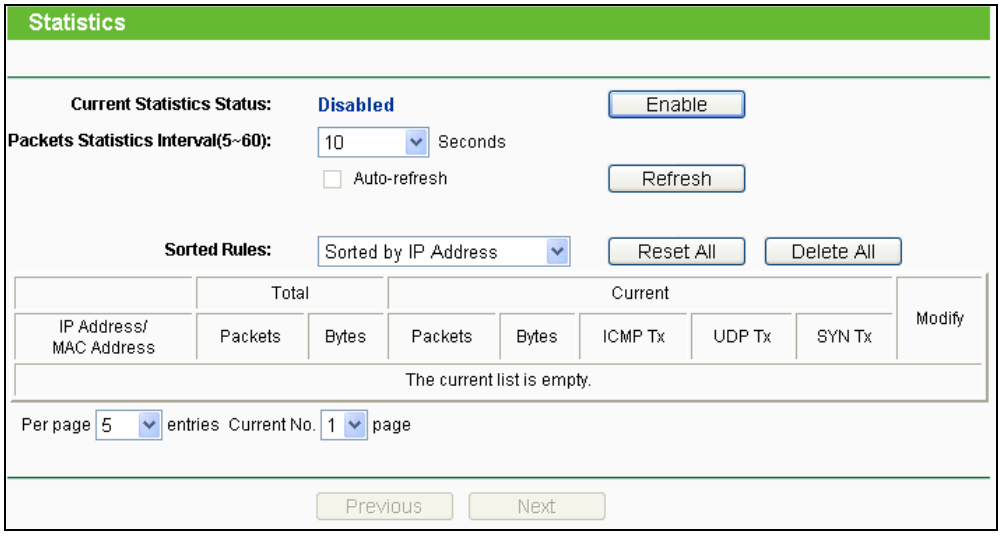


Figure 5-89 Statistics

The Statistics page shows the network traffic of each PC on the LAN, including total traffic and the value of the last **Packets Statistic interval** in seconds.

- **Current Statistics Status -** Enabled or Disabled. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will be disabled.
- **Packets Statistics Interval -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sorted Rules -** Choose how displayed statistics are sorted.

Click the **Auto-refresh** checkbox to refresh automatically.

Click the **Refresh** button to refresh the page.

Click the **Reset All** button to reset the values of all entries to zero.

Click the **Delete All** button to delete all entries in the table.

Statistics Table

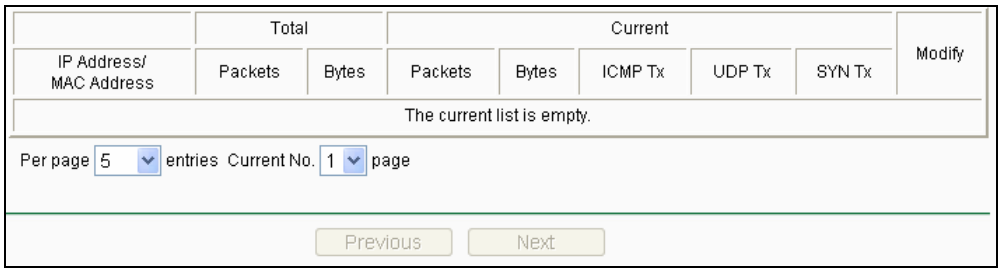


Figure 5-90 Statistics Table

- **IP Address/MAC Address -** The IP Address and MAC address are displayed with related statistics.
- **Total**
 - **Packets -** The total number of packets received and transmitted by the Device.
 - **Bytes -** The total number of bytes received and transmitted by the Device.
- **Current**
 - **Packets -** The total number of packets received and transmitted in the last Packets Statistics interval seconds.
 - **Bytes -** The total number of bytes received and transmitted in the last Packets Statistics interval seconds.
 - **ICMP Tx -** The number of ICMP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
 - **UDP Tx -** The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
 - **TCP SYN Tx -** The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
- **Modify**
 - **Reset -** Reset the values of the entry to zero.
 - **Delete -** Delete the existing entry in the table.

Appendix A: FAQ

1. How do I configure the Device to access the Internet by ADSL users?

1) First, configure the ADSL Modem configured in RFC1483 bridge model.

2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Device. The telephone cord plugs into the Line port of the ADSL Modem.

3) Login to the Device, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.

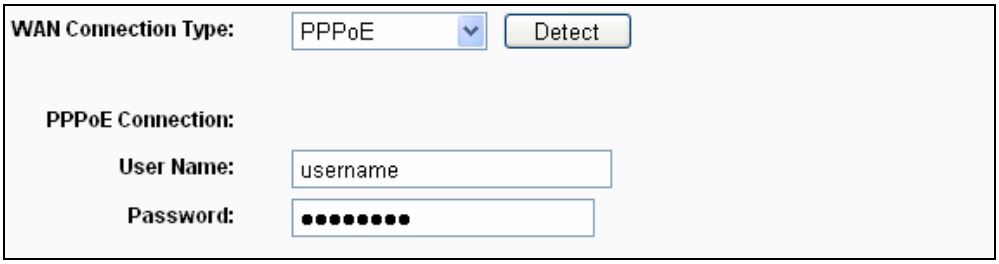


Figure A-1 PPPoE Connection Type

4) If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “Connect Manually” for the Internet connection mode. Type in an appropriate number for “Max Idle Time” to avoid wasting paid time. Otherwise, you can select “Auto-connecting” for the Internet connection mode.

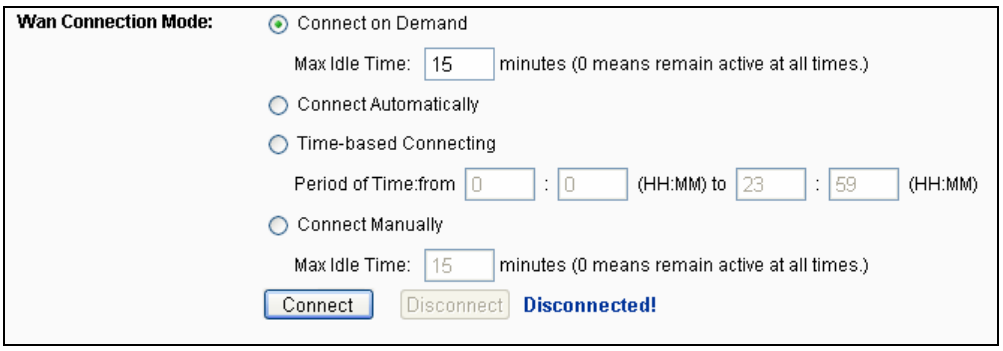


Figure A-2 PPPoE Connection Mode

Note:

1. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

2. If you are a Cable user, please configure the Device following the above steps.

2. How do I configure the Device to access the Internet by Ethernet users?

1) Login to the Device, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “Dynamic IP” for "WAN Connection Type", finish by clicking “Save”.

2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the Device and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC’s MAC address is proper MAC address, click the "Clone MAC Address" button and your PC’s MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

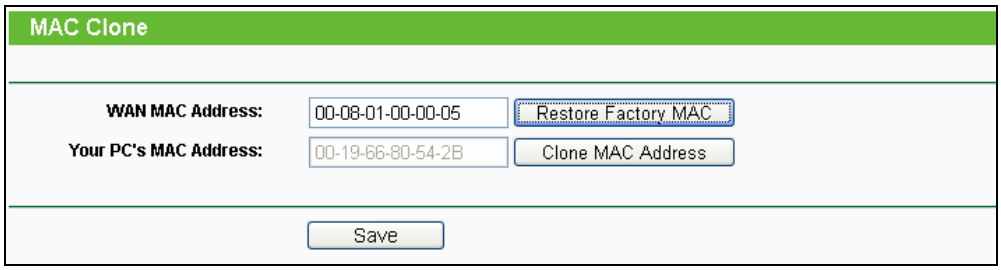


Figure A-3 MAC Clone

3. If I want to use Net meeting, what do I need to do?

1) If you start Net meeting as a sponsor, you don’t need to do anything with the Device.

2) If you start as a response, you need to configure Virtual Server or DMZ Host.

3) How to configure Virtual Server: Login to the Device, click the “Forwarding” menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New,** then on the “Add or Modify a Virtual Server” page, enter “1720” into the blank behind the “Service Port”, and your IP address behind the IP Address, assuming 192.168.1.169 for an example, remember to “Enable” and “Save”.



Figure A-4 Virtual Servers

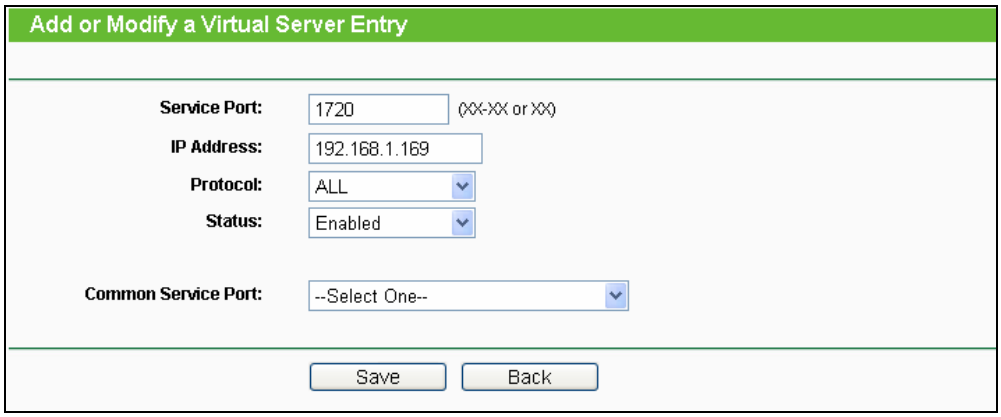


Figure A-5 Add or Modify a Virtual server Entry

Note:

Your opposite side should call your WAN IP, which is displayed on the “Status” page.

4) How to enable DMZ Host: Login to the Device, click the “Forwarding” menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click “Enable” radio and type your IP address into the “DMZ Host IP Address” field, using 192.168.1.169 as an example, remember to click the **Save** button.

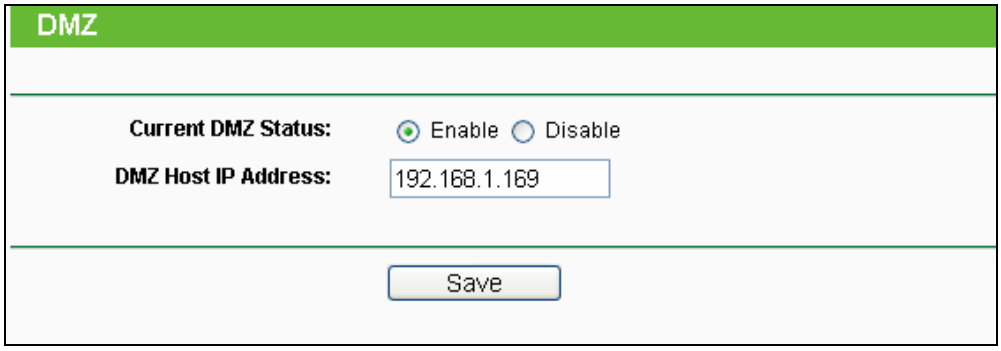


Figure A-6 DMZ

4. If I want to build a Web Server on the LAN, what should I do?

1) Because the Web Server port 80 will interfere with the Web management port 80 on the Device, you must change the Web management port number to avoid interference.

2) To change the Web management port number: Login to the Device, click the “Security” menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click “Save” and reboot the Device.

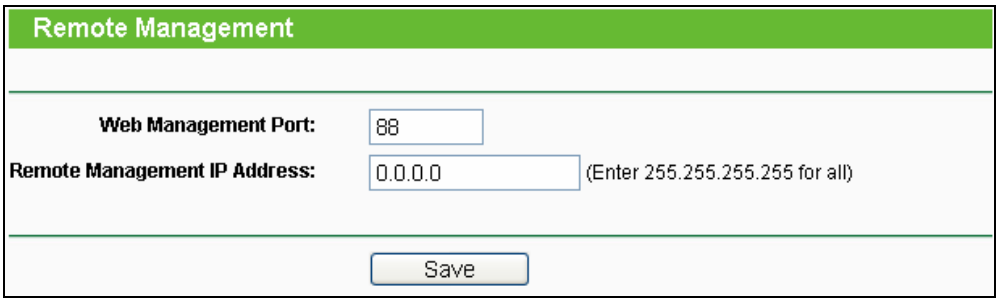


Figure A-7 Remote Management

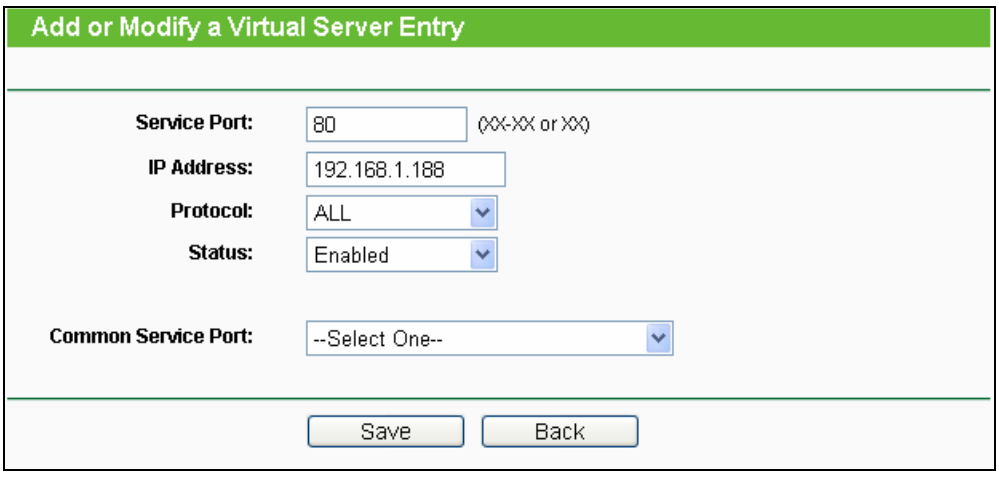
Note:

If the above configuration takes effect, to configure to the Device by typing http://192.168.1.254:88/ (the Device's LAN IP address: Web Management Port) in the address field of the Web browser.

3) Login to the Device, click the "Forwarding" menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New,** then on the "Add or Modify a Virtual Server" page, enter "80" into the blank behind the "Service Port", and your IP address behind the IP Address, assuming 192.168.1.188 for an example, remember to "Enable" and "Save".



Figure A-8 Virtual Servers



A-9 Add or Modify a Virtual server Entry

5. Why is it that the wireless stations cannot connect to the Device?

1) Make sure the "Wireless Router Radio" is enabled.

2) Make sure that the wireless stations' SSID accord with the Device's SSID.

3) Make sure the wireless stations have the right KEY for encryption when the Device is encrypted.

4) If the wireless connection is ready, but you can't access the Device, check the IP Address of your wireless stations.

Appendix B: Factory Defaults

Item	Default Value
Common Default Settings	
Username	admin
Password	admin
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Wireless	
SSID	TP-LINK_XXXXXX
Wireless Security	Disable
Wireless MAC Address Filtering	Disable
DHCP	
DHCP Server	Disable
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Address Lease Time	120 minutes (Range:1 ~ 2880 minutes)
Default Gateway (optional)	0.0.0.0
Primary DNS (optional)	0.0.0.0
Secondary DNS (optional)	0.0.0.0

Note:

The default SSID is TP-LINK_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address). This value is case-sensitive.

Appendix C: Specifications

General	
Standards and Protocols	IEEE 802.11a, IEEE 802.11n, IEEE 802.3, IEEE 802.3u, IEEE 802.1x, IEEE 802.3x, IEEE 802.11i, IEEE 802.11e
Safety & Emission	FCC, CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port, supporting passive MDI/MDIX
LEDs	PWR, LAN, four RRSI
Wireless	
Channel	36, 40, 44, 48, 149, 153, 157, 161, 165
Frequency Band	5.180 ～ 5.240GHz; 5.745 ～ 5.825GHz
Antenna	Type: External Antenna
	Gain: 15dBi
Wireless Data Rates	11a: 54/48/36/24/18/12/9/6Mbps 11n: up to 150 Mbps
Data Modulation	11a: OFDM； 11n: QPSK,BPSK,16-QAM,64-QAM
Wireless Encryptions	WPA/WPA2; 64/128/152-bit WEP; TKIP/AES
Physical and Environment	
Temperature	Operating: -30℃ ～ 70℃
	Storage: -40℃ ～ 70℃
Humidity	Operating: 10% ～ 90% RH, Non-condensing
	Storage: 5% ～ 90% RH, Non-condensing
Output Voltage	12V/1A

Appendix D: Glossary

- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**Dem**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **-** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DoS** (**D**enial **o**f **S**ervice) **-** A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi -** is a trademark of the Wi-Fi Alliance, founded in 1999 as Wireless Internet Compatibility Alliance (WICA), comprising more than 300 companies, whose products are certified by the Wi-Fi Alliance, based on the IEEE 802.11 standards (also called Wireless LAN (WLAN) and Wi-Fi). This certification warrants interoperability between different wireless devices.
- **WISP - Wireless Internet Service Providers** (**WISPs**) are Internet service providers with networks built around wireless networking. The technology used ranges from commonplace Wi-Fi mesh networking or proprietary equipment designed to operate over open 900MHz, 2.4GHz, 4.9, 5.2, 5.4, and 5.8GHz bands or licensed frequencies in the UHF or MMDS bands.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.